NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING SOCIAL MEDIA TO ENGAGE THE PUBLIC IN HOMELAND SECURITY

by

Jody Woodcock

September 2009

Thesis Advisor:	Robert Josefek
Second Reader:	Christopher Bellavita

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Leveraging Social Media to Engage the Public in Homeland Security		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jody Woodcock			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

We live in disparate times. There seems to be an increase in the occurrence of natural disasters and acts of terrorism, creating an increased dependence on government services and emergency responders. By contrast, public safety budgets are shrinking and there are fewer resources to address this greater, widespread need. The answer may be what homeland security officials have yet to do—engage the public as a full partner.

A relatively new concept has emerged in which social media or Web 2.0 tools can be utilized to facilitate the timely and accurate exchange of information and better engage the public. This thesis examines the current use of Web 2.0 technologies and crisis informatics and seeks to discover how existing social media can be used to engage the public in homeland security and emergency management.

This thesis concludes that social media connects people and helps build communities. Unfortunately, public safety officials have not embraced Web 2.0 technologies and are missing a great opportunity to engage the public and harness its collective power. With virtually no capital investment, public safety agencies can create an innovative partnership by capitalizing on tools the public uses everyday.

14. SUBJECT TERMS	**15. NUMBER OF PAGES**
Citizen Engagement, Web 2.0, Social Media, Social Networking, Twitter, Blogs, Emergency Management, Homeland Security, Communications, Crisis Informatics, Preparedness, Response, Recovery, Fear, Panic, California Wildfires, Virginia Tech, OGMA, Trust. Two Way Communications, NIMS, Incident Command, Wikis, Information Sharing, Israel, Networked Homeland Security, Public Information, Emergent Behavior, Crisis, Disaster	131
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

LEVERAGING SOCIAL MEDIA TO ENGAGE THE PUBLIC IN HOMELAND SECURITY

Jody Woodcock
Program Manager, Pierce County Department of Emergency Management, WA
B.A., Pacific Lutheran University, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: Jody Woodcock

Approved by: Robert Josefek
Thesis Advisor

Christopher Bellavita
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

We live in disparate times. There seems to be an increase in the occurrence of natural disasters and acts of terrorism, creating an increased dependence on government services and emergency responders. By contrast, public safety budgets are shrinking and there are fewer resources to address this greater, widespread need. The answer may be what homeland security officials have yet to do—engage the public as a full partner.

A relatively new concept has emerged in which social media or Web 2.0 tools can be utilized to facilitate the timely and accurate exchange of information and better engage the public. This thesis examines the current use of Web 2.0 technologies and crisis informatics and seeks to discover how existing social media can be used to engage the public in homeland security and emergency management.

This thesis concludes that social media connects people and helps build communities. Unfortunately, public safety officials have not embraced Web 2.0 technologies and are missing a great opportunity to engage the public and harness its collective power. With virtually no capital investment, public safety agencies can create an innovative partnership by capitalizing on tools the public uses everyday.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am so happy to have this opportunity to publicly thank all of the people who have had such a positive impact on my professional and personal life. First, thank you to all of the instructors and staff with the Center for Homeland Defense and Security. I truly believe the work you do every day will make our nation a safer one.

Thank you to my thesis advisor Bob Josefek. You really challenged me to find a focus to my Web 2.0 research and supported me through those many moments when the path forward did not seem so clear. To Chris Bellavita, thank you for always reminding me the most important assets to the United States are the people who live within its borders. You made me feel my quest to engage the public was a noble effort.

I want to offer a tremendous thank you to my family. To my parents, Jerry and Diane, I thank you for always encouraging and supporting me. To my husband Don, there are no words adequately to thank you for your understanding, patience and support. Finally, to the four-legged children who lay at my feet while writing this thesis—yes, I'm done and we can go for a walk now!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

We live in disparate times. There seems to be an increase in the occurrence of natural disasters and acts of terrorism around the world, creating an increased dependence on government and professional emergency responders. By contrast, public safety budgets are shrinking, and there are fewer resources to address this greater, widespread need. The answer may be found in the thing homeland security officials have not been able to do—engage the public as a full partner in emergency management and homeland security.

There has been much attention paid to preparedness in the form of Ready.gov and other local programs, but they all promote the same concept of putting together an emergency kit and waiting for the next disaster. With the development of social media, we now have the best possible opportunity to engage the public with little or no impact on fragile government budgets. The public needs information to make decisions regarding their safety. The researcher argues the public safety needs information from the public to prevent terrorism, as well as prepare for, respond to and recover from all types of disasters. The problem is ultimately a lack of trust. It is very difficult to trust those with whom you do not have a relationship, and homeland security does not have a relationship with the public.

The Basic Guidance for Public Information Officers (PIOs), as outlined by the National Incident Management System, is an example of the problem. For 25 pages, FEMA identifies how PIOs should organize and push information out to the public (FEMA, 2007). The document does not mention that the public may have critical information that the PIOs need to draw from the public and share with other public safety officials. Some jurisdictions are testing the use of social media, but many are still using the one-way communication model supported in the FEMA guidance. Few are fully engaging the public, and engaging them in all phases of emergency management, from prevention to recovery.

In 2004, the Council for Excellence in Government conducted a series of nationwide town meetings, during which they discovered information sharing was the top concern at almost every gathering. Americans are ready and willing to participate in homeland security, and there is a great need to enhance information sharing because they do not feel current systems serve their needs. As noted in the National Strategy for Homeland Security (2007), our entire nation shares a common responsibility in homeland security, and the citizens, specifically, must share in prevention and protection measures. We have sounded the alarm about terrorism but have provided no meaningful role or guidance regarding how to respond to the threat (Flynn, 2008). Citizens are, in fact, the very targets that terrorists seek. It is assumed that both the first preventers and first responders are likely to be civilians, but there is no system in place for Homeland Security officials and responders to capitalize on the public's knowledge.

Homeland security and emergency response leaders often struggle over when to release information to the public and honestly, do not seek feedback them because they do not trust their response to emergencies (Stephenson, 2007). This stereotypical portrayal of a panicked public is what makes it difficult for policy makers and local planners to include the citizens when crafting thoughtful response plans and procedures that could ultimately shape the way a disaster unfolds (Stephenson, 2007). Officials utilize a one-way approach to sharing information, yet a majority of incident After Action Reports (AAR) document frustration with achieving situational awareness during the response phase. Stephenson hypothesizes that drawing information from the public through a two-way communication system would help achieve this much-desired awareness. Public safety officials have chosen not to involve citizens to multiply their eyes and ears by potentially millions and attempt to close this situational awareness gap (Flynn, 2008). Residents have the ability to provide officials with first-hand observations, photos and video, and could direct responders to where they are most needed. Ultimately, this would allow officials to potentially make better decisions.

The University of Colorado calls this information sharing activity "Crisis Informatics" (Palen, Vieweg, Sutton, Liu & Hughes, 2007). It is a documented phenomenon that illustrates how people use social media through computers, cell phones

and other personal devices to provide, seek and broker information in times of emergency (Palen et al., 2007). The 9/11 Commission Report recommended this type of decentralized network model for sharing information and suggests government may need to consider unprecedented and fundamental changes in the way that information is collected, analyzed and used. Because public safety officials are accustomed to command-and-control and one-way information dispersal, public safety officials are not familiar or comfortable with the aforementioned concepts (Stephenson, 2007).

Leveraging Web 2.0 technologies would provide homeland security officials with enhanced situational awareness would facilitate and strengthen national priority 3.2.1, Strengthening Information Sharing and Collaboration Capabilities (HSPD 8). The public is ready to respond, not just prepare. In 2004, the Council for Excellence in Government conducted a series of nationwide town meetings, during which they discovered information sharing was the top concern at almost every gathering. Associated polling show Americans are ready and willing to participate in homeland security and there is a great need to enhance information sharing because they do not feel current systems serve their needs (Council for Excellence in Government, 2004). There is an apparent lack of trust in government and likewise, government may not trust the public's response to crisis. Regardless, reports indicate that individuals are sharing situational awareness without the involvement of government. The key is to capitalize on what is already being used and behavior that is already documented (Stephenson & Bonabeau, 2007). Networked personal communication devices and applications that the general public can and will use in a disaster offer the possibility of a new networked strategy that will allow jurisdictions to strengthen information sharing and collaboration capabilities..

Homeland security officials may have a great opportunity to expand on the crisis informatics concept by creating networked homeland security that addresses the aforementioned factors by utilizing increasingly networked mobile devices, involving users to capitalize on these devices' power through social networks. There is also potential benefit to incorporating "emergent behavior" which means groups are capable

of higher collaborative thought and behavior than individuals (Byrne & Whitmore, 2008). The bottom line is that these elements could build a system that empowers people and promotes the creative use of technology.

A. RESEARCH QUESTIONS

This thesis examines the current use of Web 2.0 technologies and crisis informatics to answer the following primary research question: *How can Web 2.0 technologies and crisis informatics be used to formulate a model that will engage and create a role for residents in Homeland Security response?*

In order to help readers understand that the public's knowledge and involvement is critical and necessary to the security of this nation and to answer this primary question, this thesis will also seek to answer the following tier of questions:

- How do residents prefer to receive homeland security or emergency information?
- How does the government currently deliver information to the public?
- What gaps exist in information-sharing models currently in use?
- Does government value the involvement of citizens in homeland security or emergency response?
- Does the American public want a role in homeland security and emergency response?
- What could American residents contribute to homeland security and emergency response?
- What could be the negative impact of involving citizens in homeland security and emergency response?

B. RESEARCH APPROACH

The research component of this thesis is qualitative. It seeks to discover how existing social media can be used to engage the public in homeland security. The intent is to discover how social media is currently used, understand the value of networked systems and provide a base of knowledge from which a model for implementation can be built.

The first step in addressing the research questions is an extensive review of existing literature. While there are not large volumes of completed research, there is some information available regarding emergent behavior, crisis informatics and how social media can leverage the wisdom of crowds. The second step is a set of interviews with public safety officials and analysis of the interviews. This group tends to be the decision-maker as to whether or not social media is to be utilized. They can be the enabler or the obstacle. The interviews help address how officials feel about the technology, their assumptions regarding public engagement and identifying barriers to implementation.

The next step involves participation in and analysis of The OGMA Workshop: Exploring the Policy and Strategy Implications of Web 2.0 on the Practice of Homeland Security. This was an invitation-only workshop consisting of Web 2.0 subject matter experts representing the categories of practitioners, behavioral science, network science and media, and technology.

The final step is synthesizing the results of literature review, interviews and OGMA Workshop to propose a model for employing Web 2.0 technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

There are four primary areas of literature that inform this research project: a group of documents that describe the foundation of social media; those that present issues related to civic engagement; studies that analyze the public's behavior during emergencies, primarily focusing on crisis informatics and emergent behavior; and models that examine how government and its citizens can become partners in public safety. While there is an abundance of material for the first three categories, there are limited examples of networked homeland security system and how government is leveraging this technology to create a bidirectional model for sharing information.

Some of the materials are primarily anecdotal. They include a series of articles that proclaim the importance of engaging the public in homeland security, but offer little statistical data. The anecdotal nature does not detract from the validity of the message, however. The views are commonly held and expressed among most Homeland Security leaders and published in national strategy documents.

A. THE FOUNDATION OF WEB 2.0/SOCIAL MEDIA

Social media connects people and information via informal networks, and is commonly referred to as Web 2.0 (Drapeau & Wells, 2009). These technologies offer organizations of all types increased agility, interoperability and effectiveness because they are not simply tools of information dispersal. They are a means for collaboration and community building and governments that harness its power could potentially interact better with citizens and anticipate emerging issues (Drapeau & Wells, 2009). After being criticized for his 88-word definition of Web 2.0, Tim O'Reilly offered the following as a second attempt:

> *Web 2.0 is the business revolution in the computer industry caused by the move to the internet as platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effects to get better the more people use them.* (O'Reilly, 2006)

Wikipedia, a Web 2.0 technology itself, offers a more expansive definition:

> *Social media is media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Social media supports the human need for social interaction with technology, transforming broadcast media monologues (one to many) into social media dialogues (many to many). It supports the democratization of knowledge and information, transforming people from content consumers into content producers. Businesses also refer to social media as user-generated content or consumer generated media.* (http://en.wikipedia.org/wiki/Social_media)

The literature makes the case that social media should be viewed as a multi-directional, interactive communication tool. For the purposes of this research, the terms social media and Web 2.0 will be used interchangeably.

1. Examples of Social Media

As shown in Figure 1, social media comes in a variety of forms and serve a variety of purposes. Wikis can be used for quick collaboration, blogs encourage interactive dialog and text messaging conserves critical resources and bandwidth (Van Leuven, 2009). Public safety officials could pick one or a variety of applications to achieve a desired outcome. The literature also suggests that social media use is on the increase. In an article published on emergencymgmt.com, Hilton Collins sited research that claims more than 300 million people visited the most popular social networking sites—Facebook, YouTube, MySpace, Flickr, and Twitter—in April 2009 alone (Collins, 2009). The study only counted each individual visitor in spite of repeat visits to the sites. An important item to remember is that Web 2.0 is not just Twitter and the technologies are not limited to the computer. They also serve most mobile communication devices (Jaeger et al., 2007).

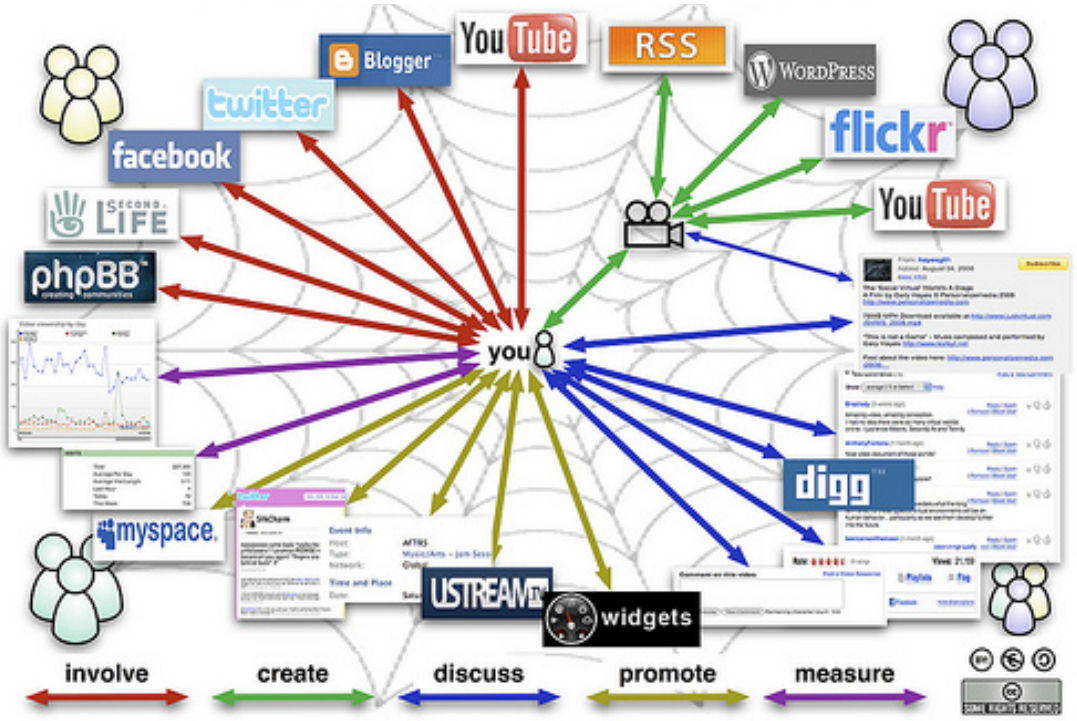


Figure 1. Graphic Representation of Social Media from flickr.com (from Hayes & Papworth, 2008)

David Stephenson identified some programs, beyond the more commonly known Twitter, Facebook and MySpace, which enable or enhance the participation of the general public:

- CUWin,
- DCERN,
- Volunteer-created Katrina wikis,
- NYC initiative to allow the public to submit photos or video for 9-1-1 or 3-1-1 calls (Stephenson, 2007), and
- Connect and Protect in Portland, Oregon.

Stephenson claims Connect and Protect seems to be the closest program to what he envisions as an effective partnership between government and U.S. residents. Journalist Gary Wolf describes his introduction to the Connect and Protect program as follows:

> *It's another day in America – talk of bird flu, issues with North Korea and the elusive Osama Bin Laden. The threat warning points to elevated and citizens are told to be vigilant. Meanwhile, other stuff is going on in Oregon. There is a hit and run, a disturbance at the Home Depot and a robbery.* (Wolfe, 2008, p. 1)

Wolfe watched this map on his computer for hours while incidents were documented and information was relayed to various members of the public. He began to wonder why millions of dollars have been invested in communications tools that do not work—this was working and was accessible to anyone who wished to participate. It struck him that if the desire was to encourage citizens to improvise and react intelligently to emergency situations; officials must provide them with information as soon as possible. Wolfe writes the key to public engagement is to capitalize on flexible Web 2.0 networks like the one he was observing on his computer monitor.

Connect and Protect uses Common Alerting Protocol (CAP) and gives precise definitions to concepts like proximity, urgency and certainty. Because warnings can be tagged with geographical coordinates, users can then customize their cell phones, pagers or other devices to get only those messages relevant to their location (see Figure 2). When considering this system, Portland officials took a closer look at their largest 9-1-1 center. They had never considered what might happen if, after collecting all those public calls, someone extracted the essentials, tagged them for easy distribution and reversed the flow of information. It was from that concept that Connect and Protect was born. A private company reformats all 9-1-1 records in CAP standard, so the impact to dispatchers in minimal if not nonexistent. Schools, security officers, the Oregon Zoo, county parole officers, property managers, libraries, and transportation companies all started to sign up. Nevertheless, this program was not just about receiving information. Almost all who receive can also send, completing the bi-directional model.

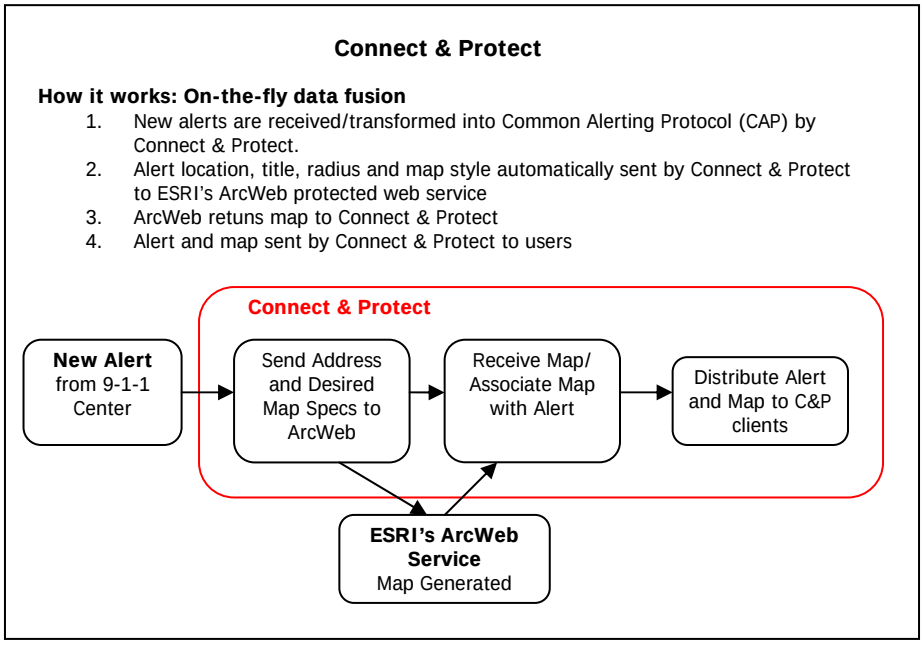


Figure 2. Connect and Protect Model (from Wolfe, 2008)

2. The Government and Web 2.0

Social media connects people and helps build communities. Not just a tool to disperse information (Drapeau & Wells, 2009), it could also provide a means for government to engage and better interact with the public. However, the literature suggests that there is a void when it comes to government leveraging existing technological systems that provide two-way communication. In fact, government agencies are globally doing a poor job of using social media (McCarty, 2008). This seems irresponsible when, according to a recent Gallup Poll, nearly half of Americans are frequent Internet users (Gallup, 2009) and as noted earlier, hundreds of thousands of people are using social networking sites (Collins, 2009). There are an increasing number of examples of government using technology to push information to the public, but there are few examples of how the public can feed information to government. It is important to understand that social media users are not just browsers or readers, but also providers and

participants (Drapeau & Wells, 2009). As W. David Stephenson was quoted, "Collaboration can be literally a matter of life and death in a disaster" (Spadanuta, 2007).

The general public may be capable of being full partners in emergency preparedness and response. In particular, people may be able to use emerging new technologies to provide otherwise unavailable situational awareness and to use existing social networks to decrease the burden on first responders (Stephenson, 2007, p.1).

B. CIVIC ENGAGEMENT: MAKING THE PUBLIC A PARTNER IN HOMELAND SECURITY

> *The nation's homeland security strategy calls on federal, state and local governments, businesses, communities and individuals throughout the country to work together to achieve a shared vision of a secured way of life … The American public has been left out and is largely missing in action.* (Bach & Kaufman, 2009, p. 1)

1. Civic Engagement on the Decline

Even after President Bush and Homeland Security Secretary Tom Ridge called on all Americans to fight terrorism post 9/11, homeland security educators and researchers Robert Bach and David Kaufman found an unprepared and uninvolved citizenry. They noted that "community engagement has been left to become a 'nice thing to do,' rather than to take its proper place as the cornerstone of effective security" (Bach & Kaufman, 2009, p. 3). They believe that the ability to fight terrorism and prepare for natural disasters will fall more squarely on the capabilities of local neighborhoods and families than on billions of dollars worth of equipment (Bach & Kaufman, 2009).

In the book *Bowling Alone*, author Robert Putnam attribute this lack of engagement to the overall decline in social connectedness. Between 1974 and 1998, the frequency with which Americans "spend a social evening with someone in the neighborhood" fell by about one third (Putnam, 2000). Even with the perceived rise in popularity of neighborhood watch groups of the past 20 years, a Department of Justice survey of 12 cities found that only 11 percent of residents had ever attended this type of neighborhood meeting (Putnam, 2000). In contrast, the same survey indicated that 14

percent of the respondents kept a weapon, 15 percent kept dogs for protection and 41 percent had extra locks installed in their homes. Putnam asserts that we invest more in guns, dogs and locks that we do in social capital (2000).

2. Web 2.0 Did Not Cause the Decline of Social Connections

Some believed the development of the Internet caused social withdrawal, but the decline started long before the Internet age. By the time that the Internet reached 10 percent of American adults in 1996, the nationwide decline in social connected and civic engagement had been underway for a least a quarter of a century (Putnam, 2000).

In fact, the opposite seems to be true because within a few years of the Internet's launch, most civic engagement could be found on line. Social networks based on electronically aided communication are thought to create virtual neighborhoods (Putnam, 2000). Putnam quotes Internet theorist Michael Strangelove to make this point,

> *The Internet is not about technology and it is not about information. It is about communication – people talking with each other, people exchanging email … the Internet is mass participation in fully bi-directional, uncensored mass communication. Communication is the basis, the foundation, the radical ground and root upon which all communities stand, grow and thrive.* (Putnam, 2000, p. 171)

At the 2009 conference for the Urban Area Security Initiative (UASI) programs, a representative from the San Francisco Department of Emergency Management noted that the old way to do business was to talk at people—the new way is to have an online conversation (Dudgeon & Hogan, 2009). The department subscribes to the belief that social media adds to public engagement by reaching larger audiences, providing meaningful dialog and building communities. Bach and Kaufman agree and suggest there must be dialog with the public about risks they face and the actions they can take (2009). Social media is an important tool to enable this engagement.

Tools initially designed for making friends in cyberspace has the capability of transforming emergency management in unexpected ways (McCarter, 2009). In addition to sharing information through Web 2.0 applications, public safety officials are able to obtain some of the most valuable sources of information for situational awareness during

crisis response—eyewitness accounts. Traditional, one-way delivery of information fails to leverage humans as sensors (Mehrotra, Butts, Kalashnikov, Venkatasubramanian, Altintas, Hariharan, Lee, Ma, Myers, Wickramasuriya, Eguchi, & Huyck, 2004). Sophia Liu, a doctoral student at the University of Colorado was evacuated from her home in Boulder, Colorado on January 7, 2009. Because she happened to study social media, she used her knowledge to share information with others. Liu used Twitter to provide updates from a variety of sources such as official Boulder press releases, local broadcast news report and eye witness accounts. Her goal was to get all of the information in one place. The goal is to leverage social media users like Liu to help share with and extract information from the public (McCarter, 2009). McCarter affirms the communication aspect of social media, writing it is more than how we reach out to the public—it is also about the public talking to public safety officials and the public talking to the public (2009).

There is great potential in Web 2.0, but trust remains an issue and a potential barrier to implementation.

3. An Issue of Trust

The issue of trust is mentioned many times throughout this thesis. Bach and Kaufman believe the problem is that "government officials and the public fundamentally misunderstand and mistrust each other" (2009, p. 2). Citizen engagement is about creating a relationship, and with that, you must have trust.

> *Interpersonal trust has been defined as the extent to which a person is confident in, and willing to act on the basis of words, actions and decisions of another. It is the glue that propels a team toward successful completion of a project*. (Altschuller & Benbunan-Finch, 2008, p. 385)

Polls show Americans are much more interested in getting involved that government officials believe, but are skeptical that the government will provide accurate information or deliver on promises. More specifically, a 2005 Harris Poll revealed that only 27 percent of those surveyed trust government (Covey, 2006). One explanation for this lack of trust is limited government engagement with the public (Bach & Kaufman,

2009). For example, Bach and Kaufman make the point that public safety agencies spend a great deal of time developing relationships with one another, but the same effort is not extended to residents. Along with the public's mistrust in government is government's mistrust of the public. The literature suggests that public officials envision individualistic acts that can go badly and are often uncomfortable with the improvisation that the public might employ (Kendra & Wachtendorf, 2006).

Stephen Flynn writes that government should take the initiative to replace the current climate of secrecy and suspicion with a climate of inclusiveness and trust (Flynn, 2007). He believes our success relies on the participation of every American, so we need to start seeing the public differently. In a *Homeland Security Today Magazine* article, Mickey McCarter supports that concept, "They [members of the public] are not passive receptacles of information where we dump information into them and hope they do what we ask. Instead, they must be viewed as active participants" (2009, p. 46).

Successful partnerships between government and its residents can be and have been achieved. Community Oriented Policing is one example from which public safety officials can draw inspiration. Over the past 20 years, Community Oriented Policing has transformed a "top down enforcement strategy into an engagement based model for public safety" (Bach & Kaufman, 2009, p. 5).

To further analyze issues of trust, the next section draws from Israel's experience with terrorism and engagement of its public. The focus is not the use of social media to engage them, but rather the approach to include the public as a full partner in prevention, preparedness, response and recovery.

4. Israel: Smart Practices for Citizen Engagement

Israel has integrated terrorism preparedness into its culture through a variety of means, creating a culture of involvement and preparedness. In contrast, most Americans are unprepared for an actual event, according to a 2005 telephone survey conducted by New York University's Organizational and Community Preparedness project. The survey

found that most Americans are unaware of their local government's plans for response and recovery and are deeply confused about what to do in the event of an actual catastrophe (Light, 2005).

Israel understands that savvy people—more than technology, physical barriers or special tactics—are the critical weapon to wield against terrorists (Lehrer, 2001). This nation that has endured long terror campaign has demonstrated that a well-informed and involved public is a vital part of developing the ability to withstand any kind of terror attack (Forest, 2006). At one point or another nearly every Israeli has take an active role in the fight against terrorism. Public participation has been one of the cornerstones of Israeli defensive measures against domestic terrorism and much of the country's success in foiling terrorist bombings can be attributed to public awareness.

Israel has made preparedness a way of life (Conroy, 2008). Fighting terrorism has been integrated into its culture through a variety of means. Children in primary schools learn about preparedness through an established educational curriculum. They learn about chemical and biological weapons, how to spot suspicious items and people, and how to use a gas mask. High school students receive addition education and training, and are then required to perform volunteer work in emergencies. Educating and training the public starting at a very young age has helped to establish this culture of preparedness.

With the unimaginable pressure of daily terrorism, some might worry that the population might take prevention measures a bit too far. However, vigilante behaviors are rare in Israel, partly because a massive corps of police volunteers allows responsible citizens to play an active role in official state security (Lehrer, 2001). While many American police departments also use volunteers, they mostly limit their participation to crowd control, administrative duties, parking enforcement and directing traffic. In Israel, the volunteer corps actually dwarfs the professional police force. For example, Tel Aviv has a little over 3,000 full-time police officers and more than 8,000 uniformed volunteers. With so many volunteers, and such well-prepared ones, they are often the first on scene to deal with attacks and other emergencies.

Every Israeli prepares for the worst. Each home built since the Gulf War has, by law, a secure room that can function as a family shelter against terrorist attack.

> *At a glance, the secure room in Uzi Landau's modest apartment near Tel Aviv looks like a typical study. A computer whirs quietly in one corner and software manuals, spiritual texts and books of political philosophy line the shelves. But a closer look tells a different story. A heavy steel plate is rolled over the window with a few tugs. The windows and steel door have gaskets which seal the room against biological and chemical attack. The walls, floor, and ceiling of the room are made of reinforced concrete. And government-distributed gas masks site beside a manual for Windows 98.* (Lehrer, 2001, p. 2)

All neighborhoods have pits into which people can throw suspicious packages that could be bombs and parents must work a few days each year providing security at their children's school. A comprehensive civil defense program provides every citizen with information about evacuation routes and shelters. Major hospitals maintain mass outdoor showers to wash off chemical weapon residue. Still, with this comprehensive approach and numerous available tools to fight a terrorist attack, Israelis have no illusions that such measures and target hardening protects them entirely from terrorism (Lehrer, 2001). Israeli communities must guard themselves. Residents in Jewish settlements along the West Bank have set up their own emergency response centers. A supervisor in one of those centers, Yiftich Sapir, said, "Bulletproof vehicles aren't enough here. You need people to respond." (Lehrer, 2001, p. 2)

As noted in the NPS Thesis titled *What is Going to Move the Needle on Citizen Preparedness?*, the application of Israeli models is difficult because of government structure, the presence of enemies on all borders and demographics and population (Conroy, 2008). Israel is slightly smaller than the state of New Jersey and has a population of approximately 6.4 million. This is compared to the U.S. population of nearly 298 million. The Israeli approach of involving every citizen in the fight against terrorism is an overwhelming task when you are dealing with almost 300 million people.

The literature suggests citizen preparedness and education must be approached from an empowering perspective, as it is in Israel. According to reporter and author Siobhan Gorman, applying lessons learned from Israel will not be effective until we

recognize that terrorism is psychological warfare and one of the best responses may to be gradually become less afraid of it (Gorman, 2003). Engaging the Israeli public in the fight against terrorism has kept the citizens from falling victim to hopelessness and the sense that they can do nothing about the threat. The vigilance of the Israeli public has played a key role in preventing terrorism. Policy analyst Jonathan B. Tucker, Ph.D., wrote that as a result of this awareness "ordinary citizens foil more than 80 percent of attempted terrorist attacks in Israel, including time bombs left by terrorists" (Tucker, 2003, p. 3).

There literature points to a problem when it comes to the application of Israeli smart practices in the United States. Americans are investing increasingly less time and effort in building and maintaining their social networks. James Forest cited author Robert Putnam's research for the book *Bowling Alone,* which states that Americans have become increasingly disconnected from family, friend and neighbors (Forest, 2006). Compared to fifty years ago, Americans belong to fewer organizations, know their neighbors less, meet with friends less frequently and even socialize with family members less often. According to Thomas A. Glass, community and family connections are exactly what are needed to fight terrorism. He notes that "preexisting personal knowledge of one another, being in a situation with people you know, inoculates against panic and dysfunctional behavior" (Glass, 2001, p. 71).

The report titled *We the People: Homeland Security from the Citizens Perspective* sums up the heart of an engagement strategy, "The greatest resource the United States has for enhancing homeland security—which has been largely untapped thus far—is the American people. There is no time like the present to establish a tradition of strong citizen involvement in Homeland Security" (Council for Excellence in Government, 2004). Further support for this idea comes from the survey conducted by New York University's Organizational and Community Preparedness Project which concludes that citizens want more than color-coded alerts and information about storing water, duct tape and plastic—they are ready for an honest conversation about what they can and should do, and the risks of inaction (Light, 2005).

One element of engaging the American people is to use what Stephenson and Bonabeau (2007) call a networked strategy. They observe that networked personal

communication devices and applications that the general public can and will use in a disaster offer the possibility of a new approach that may allow jurisdictions to strengthen information sharing and collaboration capabilities. This approach can also enhance a public engagement strategy.

C. PSYCHOLOGICAL RESPONSE TO DISASTER: FEAR, PANIC AND THE IMPACT OF INFORMATION

The previous section examines literature that suggests public officials do not trust the public's emergency response capabilities. Researchers link this lack of trust to the assumption that individuals will panic in the face of danger (Ripley, 2008; Sutton, Palen & Shklovski, 2008; Vieweg, Palen, Liu, Huges & Sutton, 2008). The fear of fear and myths of panic remain barriers for government to engage new approaches to information sharing. For that reason, this section examines fear, panic and the idea that sharing information may reduce the likelihood or degree of either response.

1. Fear

What does it feel like to face death? What happens in our brains when the ground rumbles and buckles beneath our feet? The most obvious answer would be fear. This is a natural, primitive reaction to crisis. Fear is a survival mechanism that has served us well, with some exceptions, through history. Author Amanda Ripley (2008) believes it is misunderstood as to how fear guides our reactions. She writes, "People's behavior in a disaster is inexplicable until we understand the effect of fear on the body and mind," (Ripley, 2008, p. 57).

In *The Unthinkable*, Ripley uses the example of a terrorist attack on the Dominican Republic's embassy in Bogota, Columbia, specifically focusing on the reaction of U.S. Ambassador Diego Asencio. She describes how fear moved through his body. At the first 90-decibel gunshot, signals traveled to Asencio's brain by way of his auditory nerve. When the signal reached his brainstem, neurons passed the information to his amygdala, an almond-shaped mass located deep within the temporal lobes that are central to the brain's fear circuit. In response, the amygdala set off a series of changes in

the body over which Asencio has absolutely no control. His blood chemistry changes, his blood pressure and heart race increased and adrenaline was released. This potentially performance-enhancing shot of hormones produces the *fight or flight* reaction.

A rule for fear, however, is that for every gift it provides, it takes one away (Ripley, 2008). We may encounter increased strength and speed, but we may lose the ability to solve simple problems or even control of our bladder. Time and space can also become disjointed as the embassy terrorist attack scenario continued. Ripley quoted Asencio, "the action around me, which seemed to speed up at first, now turned into slow motion. The scene was like a confused, nightmarish hallucination, a grotesque charade. Everything I saw seem distorted; everyone, everything was out of character," (Ripley, 2008, p. 60). Ripley's research shows that many reported similar reactions as they evacuated from the World Trade Center on September 11, 2001. Ripley reminds her readers that the human body is hard-wired for a fear response, but it does not equal panic (Ripley, 2008).

2. Panic

We must understand there is panic, the emotion, and panic, the behavior. Panic behavior is defined as "irrational, groundless or hysterical flight that is carried out with complete disregard for others" (Auf der Heide, 2004, p. 342). Many disaster victims report they panicked, but in truth, they did not misbehave. It was likely the fear response they were experiencing (Ripley, 2008).

Social epidemiologist Dr. Thomas Glass wrote, "Panic happens in disaster movies, but typically not it real disasters" (2001, p. 71). In an article Glass co-wrote with Monica Schoch-Spana (2002), it was noted there is an assumption that the general public tends to be irrational, uncoordinated and uncooperative in emergencies—not to mention prone to panic. The University of Delaware's Disaster Research Center studied more than 500 events and found panic was of very little practical or operational importance (Auf der Heide, 2004). What they did find was people became involved in protective activities, such as warning others, calling for help or assisting with rescue. Glass's research backs up the University of Delaware studies. On the basis of observations and random

interviews of 415 people in the World Trade Center stairwells, he found there was little panic and people were cooperative (Glass, 2001).

These studies do not show, however, that panic never exists. Panic can occur if and only if three conditions exist (Ripley, 2008). First, the person must feel trapped. Second, he must have a sensation of great helplessness and finally, he must have a sense of profound isolation. Panic can most commonly be found in large crowds, such as the yearly hajj where people have died in stampedes. The crowd can be calm and well mannered but if humans have less that one square yard of space, they lose the ability to control their movement (Ripley, 2008). This loss of control can create the opportunity for the three conditions of panic to exist, but again these cases are rare.

Even before a disaster occurs, the people in charge use panic as an excuse to discount the public. People will panic—the legend says—so we cannot trust them with the information or training. Ripley quotes noted disaster expert Dennis Mileti, "Do you know how many Americans have died because someone thought they would panic if they game them a warning? A lot!" (Ripley, 2008, p. 157).

The literature strongly suggests that people respond to crisis creatively and with collective resourcefulness. Ripley claims if regular people got as panic stricken in a crisis as most of us think they would, Flight 93 would have certainly destroyed the White House or U.S. Capitol (Ripley, 2008). It was assumed that air raids in Britain during World War II would panic the public. When the bombs did fall, Britain's residents reacted unexpectedly. At the time, a writer from a local newspaper noted, "these were either the calmest or stupidest people in the world," (Ripley, 2008, p. 149). Similarly, it was assumed that residents near 3-Mile Island in Pennsylvania would panic, but they reacted calmly and evacuated in an orderly manner (Ripley, 2008).

3. Information Sharing Reduces Fear

People experience fear in a crisis, but rarely panic. They, in fact, respond with great skill and innovation. So the question is how do we keep fear to a minimum and harness the skill of the general public to respond to disasters and protect the homeland? One answer is sharing information. Ripley quoted former FEMA Director James Lee

Witt to this point. He said, “What I’ve always found is that people will respond to meet a need in crisis if they know what to do” (Ripley, 2008).

Our bodies are hardwired to experience the emotion of fear but we can reduce its impact through information and training. Ripley wrote, “The actual threat is not nearly as important as the level of preparation. The more prepared you are, the more in control you feel and the less fear you will experience” (Ripley, 2008, p. 70). Glass agreed and wrote that information and practice can reduce fear—just know where the stairs are gives your brain an advantage. Research into plan crashes has similarly found that people who read the safety cards are more likely to survive (Glass, 2001).

Glass wrote, “Our tendency is to withhold information too long for fear that it will cause panic when, in fact, it is the absence of information that is most likely to cause panic” (Glass, 2001). Officials must recognize that people can be trusted to do their best at the worst of times. Emergency managers often miss the opportunity to harness the capacities of the civilian population to enhance the effectiveness of large-scale emergency response (Ripley, TIME, 2001). Glass and Schoch-Spana (2002) believe that this power can be secured through information and that providing information is as important as providing medicine. “In the face of uncertainty, the general public would need reassurance, descriptions of the response measures under way, instruction in personal and collective protective measures and messages of hope” (Glass & Schoch-Spana, 2002, p. 220). It is difficult to provide that level of detail in a twenty-second sound byte on the evening news. An option to provide this level of specificity is using social media. This remote, mobile form of communication is critical when traditional media outlets are not available, reliable or applicable. A mechanism for feedback, which social media has, is a critical part of creating a partnership with the public (Glass & Schoch-Spana, 2002).

Typically, the initial response to warnings of disaster is disbelief, not panic. If it appears a warning is credible, the next response is to try to confirm its validity by listening to the radio, watching television or going on-line to chat with friends and relatives (Auf der Heide, 2004). In a crisis, people believe information is empowering and not knowing is far worse that knowing (CDC). In a risk communication pamphlet,

the CDC notes that when people are swamping emergency hotlines or overloading email boxes and websites, they are not panicking, they simply are seeking the information they believe they need. Detail is critical. For example, a broadcast warning that the river will crest 10 feet above flood stage may convey less meaning than providing maps to show the flooded areas or to identify landmarks that might be under water. By utilizing social media, emergency officials can release consistent messages in real-time and address any rumors. Failing to do so could compromise any operational success.

By providing information, emergency officials can help manage fear and engage the public. It is also believed this practice can greatly reduce the number of psychological casualties in a disaster (National Academy of Science, 2003). In addition to communicating information about the incident, it is also important to provide information regarding the range of potential psychological responses they might experience and how to get assistance. Disaster researchers recommend that plans be based on what people naturally tend to no and to not force people into a command-and-control world (Auf der Heide, 2004). If people naturally want more information to calm their fears and get involved, then officials should provide a way to make that happen. Social media is an excellent option.

D. ENGAGEMENT MODELS

There are a variety of ways to engage the public in homeland security and emergency management, as well as examples of how it is already being done. To begin, the following section provides a comparison of centralized and decentralized networks in the context of citizen engagement. With that background, the remaining sections highlight how individuals are already engaging each other through crisis informatics and how that can be applied to the concept of networked homeland security.

1. Centralized v. Decentralized Networks

Before presenting the details of networked homeland security and crisis informatics, it is important to understand the concept of networks. First, there is the centralized network that is typically employed by any business or government agency.

There is often an institution organization chart that identifies a clear leader, management, supervisors and staff—roles are clearly delineated and it provides for a specific way to make decisions (Brafman & Beckstrom, 2006). The researcher's employer is no exception as indicated by the following chart:

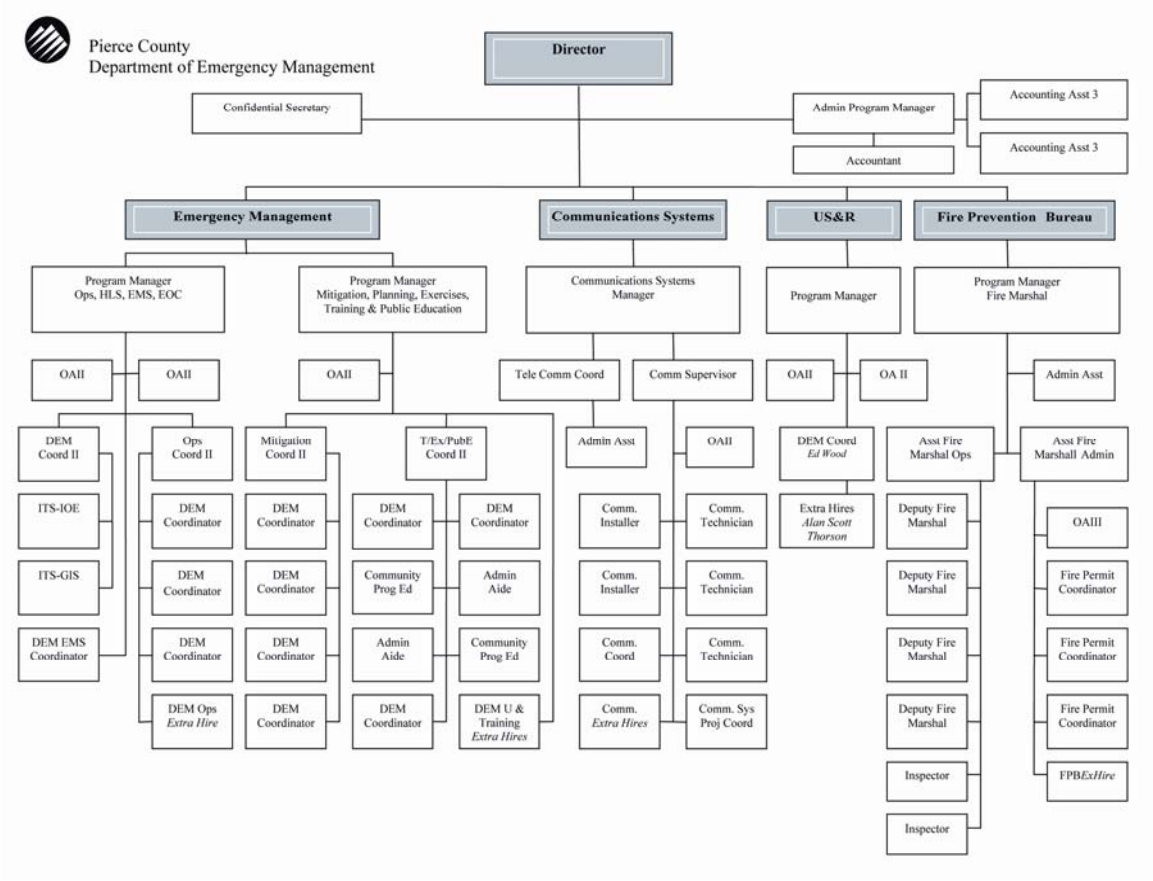


Figure 3. Pierce County Emergency Management Organizational Chart

According to Brafman and Beckstrom's book *The Starfish and the Spider* (2006), this top down network is compared to a spider. "If you chop off the spider's head, it dies. It could maybe survive without a leg or two, but it certainly couldn't survive without its head" (Brafman & Beckstrom, 2006, p. 34). The same can be said about the federally mandated Incident Command System which utilizes a modular structure to identify Command, Operations, Planning, Logistics and Finance/Administration. By contrast,

social media is more like a starfish, which has no head. It represents a decentralized network of nodes and links that are not connected through hierarchy (see Figure 4).

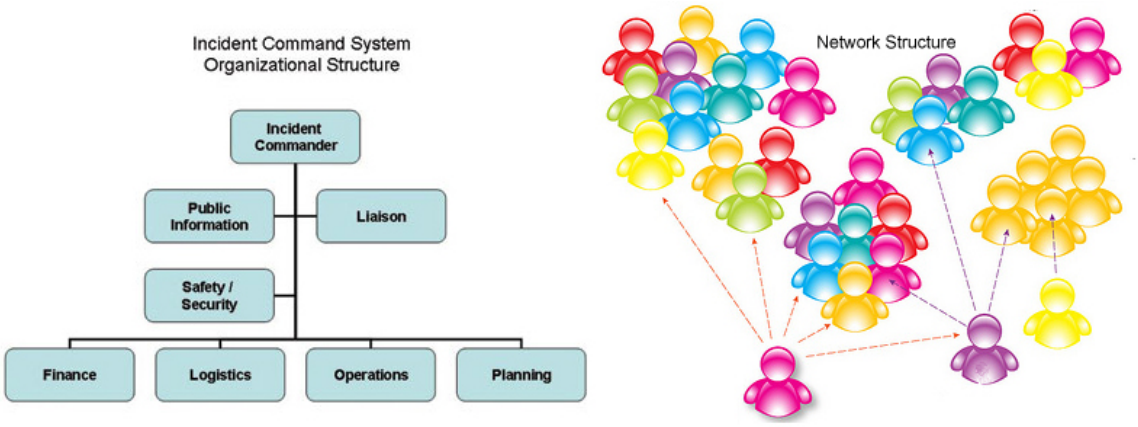


Figure 4. Spider versus Starfish Organizations (from Brafman & Beckstrom, 2006)

Brafman and Beckstrom claim that decentralization has been lying dormant for years, but the advent of the Internet has unleashed this force (2006). This does not mean that leaders will not emerge, but if they do, they have little power over others (Brafman and Beckstrom, 2006). “The absence of structure, leadership and formal organization, once considered a weakness, has become a major asset. Seemingly chaotic groups have challenged and defeated established institutions. The rules of the game have changed” (Brafman & Beckstrom, 2006, p. 7)

To further compare the two types of networks, in a top-down organization the leaders want to control what is happening and this may limit creativity (Brafman & Beckstrom, 2006). A decentralized organization empowers it membership and enjoys a high tolerance for innovation (Brafman & Beckstrom, 2006). In the Starfish and the Spider, the authors offer the following quote from EBay to make the point: “We believe people are basically good. We believe everyone has something to contribute. We believe that an honest and open environment can bring out the best in people” (2006, p. 163). The EBay example is unique because it is not a starfish—even though it hosts a user to user

network. It represents what is known as “the combo special” or the hybrid organization (Brafman & Beckstrom, 2006). A business like EBay must have structure and accountability to promote trust, but it shows that a spider can launch a starfish movement. Similarly, government can keep its organizational hierarchy but also embrace the use of decentralized networks like Web 2.0.

Social media decentralized networks represent the strength of weak ties. In *Megacommunities*, the authors quote Stanford professor Mark Granovetter to define this concept, “this means it isn’t necessary to know someone deeply or even well to allow for the exchange of information that makes the whole network more productive” (Gerencser et al., 2008, p. 72). He continues by explaining that people with many weak ties are often better informed and better equipped to share information than those with fewer strong ties to close friends and family (Gerencser et al., 2008). Web 2.0 can provide a network of bridges that allow people to receive news or other important information earlier that those with only strong ties. The authors also argue that those with weak ties can organize more quickly to take action (Gerencser et al., 2008). The variety of social media tools can be used to enhance this network and enable continual engagement of weak ties, or decentralized networks, through texting, instant messaging or mobile phone blogging (Gerencser et al., 2008).

The concept of networks provides evidence as to why government is having difficulty fully embracing social media to engage the public. A centralized network is not set up to easily launch decentralized movement (Brafman & Beckstrom, 2008). A decentralized network of weak ties promotes innovation and improvisation. Improvisation is defined as a distinct capacity that people have to address what needs to be done rather than what ought to be done (Kendra & Wachtendorf, 2006). In fact, emergency managers spend a great deal of time planning and using the Incident Command System to prevent improvisation because it suggests un-trusted and potentially unexpected actions. To the contrary, the reality of an event does not necessary fit the plan.

For example, the waterborne evacuation of Lower Manhattan after 9/11 was improvised. Several thousands of people were evacuated by an assortment of vessels—

tow boats, dinner cruise boats, yachts. This was not a matter of inadequate plans; there were no plans, so this decentralized group of weak ties saw the need to response and found a way to work together (Kendra & Wachtendorf, 2006).

When it comes to using Web 2.0 to engage the public in homeland security, it is critical to find a way to become a hybrid organization. The utility of the community should not be underestimated. While we hear the need for better command and control and a coordinated use of resources, this can be achieved through a decentralized network that has no command or control context (Kendra & Wachtendorf, 2008). The following sections will provide specific examples.

2. Crisis Informatics

The University of Colorado has produced most of the scholarly literature related to how citizens engage with one another through social media. In fact, its researchers coined the phrase "crisis informatics." The University of Colorado researchers define the activity of crisis informatics as a documented phenomenon that illustrates how people in and out of the disaster go on line through computers using Web 2.0 applications, cell phones and other personal devices to provide, seek and broker information in times of emergency (Palen, Vieweg, Sutton, Liu & Hughes, 2007). Opportunities and mechanisms for participation by members of the public are expanding the information arena of disasters. This body of work provides specific examples of how networked personal communication devices and applications are tools that the general public can and will use in a disaster. The research team provides great detail of the public's use of Web 2.0 technologies during the Virginia Tech shooting and the California wildfires.

a. Virginia Tech

As the world tuned to CNN and other media outlets in April 2007 to watch the unfolding of the Virginia Tech shooting, researchers at UC noted that thousands were logged on to another information source—Facebook.com and they documented the actions described in the rest of this paragraph (Palen et al., 2007). Within 30 minutes, students in a journalism class started posting information to a class Web site. After the

second shooting was publicized, the information seeking became more aggressive and moved online to Facebook, MySpace and Wikipedia. Students, family members and loved ones started using text messaging and instant messaging (IM) to check the safety of others. Large groups could be contacted in a short amount of time. If someone's IM buddy was active, it meant that person was online and was okay. Groups on Facebook connected thousands of people.

Through a series of interviews, researchers determined the lack of official information so the public went to the device they use every day. They also discovered that, contrary to popular opinion; crisis informatics did not lead to rumor mongering or the spread of misinformation, which government officials often attribute to citizens (Palen et al., 2007). In fact, between Facebook, Wikipedia and others, all 32 victims were accurately identified before they were officially release by the school. Even though the lists were compiled in different sequences, they were never wrong. It is believe that adding a name to the list was taken very seriously, so participants self policed. Another University of Colorado study suggests that disaster situations have demonstrated, throughout history, that people rise to difficult challenges to help others often through remarkable innovations and adaptations of their own abilities and resources (Vieweg, Palen, Liu, Hughes & Sutton, 2008). One of these adaptations in the case of Virginia Tech was collective intelligence where a large distributed group of people exhibit problem-solving capabilities. They just did it on line.

b. Southern California Wildfires

The University of Colorado researchers continued their work during the 2007 Southern California wildfires, which provide another example of non-routine events resulting in non-routine behaviors. They monitored Web 2.0 technology to analyze how and why people and organizations leveraged their own social networks to find and provide information outside of the official response effort. In California, like most of the nation, planning efforts focused almost solely on the role of official response and the management of public activities. Public or peer-to-peer communication was not considered legitimate (Sutton, Palen, & Shklovski, 2008).

The researchers wanted to understand why crisis informatics was necessary and suggested one problem might be traditional command and control. The Incident Command System (ICS) was developed in response to major California wildfires in the 1970s. While it manages command and control, it also manages the flow of information within and between official response agencies and the media, ignoring the fact that studies show people seek information from a variety of sources. Government tends to focus on the unidirectional model. Public officials tend to view peer-to-peer communication as "backchannel," meaning it has the strong potential to spread misinformation and rumor, thereby compromising public safety (Sutton et al., 2008). Studies have shown the opposite is true, that backchannel efforts are often critical and accurate, and provide a way to actively engage in public safety (Sutton et al., 2008).

During the 2007 wildfires, researchers reported that people used a variety of means to seek information. Local media was considered important but often lacked specificity for a certain area, was biased toward the large metropolitan areas, tended to focus on the sensational or was simply inaccurate (Sutton et al., 2008). Study respondents reported that official government Web sites were slow to update and considered relatively useless. Not only did people seek information, but also 36 percent of the respondents said they posted information. Some reported a need to contribute to allow them to better cope with the situation. Community information sites like rimoftheworld.net and signonsandiego.com were considered critical during response and recovery efforts.

While it is difficult to prove that disaster response is any better or worse because of crisis informatics, this literature shows it does have an impact. The document not only describes in detail how people think collectively and share information, but also why people feel this activity is necessary. People in and out of the disaster go on line through computers, cell phones and other personal devices to provide, seek and broker information. Randall J. Larsen, retired Colonel in the U.S. Air Force and Director of the Institute for Homeland Security, notes that government has spent billions of dollars on high-tech communications equipment that become damaged or unusable. An example is in the case of Hurricane Katrina, when the equipment was under water. Another is

between organizations that do not want to speak to each other, as in the case of New York Police and Fire (Larsen, 2007). This literature suggests the answer may be something right under our collective noses.

3. Networked Homeland Security

The passengers aboard United Airlines Flight 93 prevented what could have been hundreds more lives lost on 9/11. Al Qaeda hijackers did not ban the use of cell phones, so they began to collect information. Through calls to loved ones, emails and text messages passengers learned the fate of the other hijacked airplanes and decided to respond and defend the White House, the United States Capitol and potentially saved hundreds, maybe thousands, of lives. Would passengers on the other flights have responded that same way if they had had the information? Homeland security and emergency response leaders often struggle over when to release information to the public and honestly, how much to involve them. There must be a way to harness the many strengths of the American public when it comes to emergency response. The theme of this research is captured in the following quote from former Homeland Security Secretary Tom Ridge:

> *As hard as homeland security professionals in the private sector and all levels of government are working to secure America, we can't get the job done without the support and help of individual citizens … We all must work together to protect our homeland.* (Council for Excellence in Government, May 2004, p.6)

This body of literature has not uncovered is why public safety officials have chosen not to involve citizens to multiply their eyes and ears by potentially millions and attempt to close an apparent emergency response gap. Some of the literature makes a case for a partnership in emergency response (Flynn, 2008; Byrne & Whitmore, 2008; Bach & Kaufman, 2009), but none offer what that partnership might look like. An option presented by David Stephenson and Eric Bonabeau is to create a role for the public that makes them an engaged partner by creating what he calls networked homeland security.

Networked Homeland Security employs the netwars theory developed by the RAND Corporation that describes a "networked organization structure of its practitioners

—many groups being leaderless—and the suppleness in their ability to come together quickly in swarming attacks" (Stephenson, 2007, p. 2). In other words, it provides a networked response to a networked enemy. David Stephenson believes this theory applies to terrorist networks and natural disasters, which exhibit similar characteristics. They strike the most vulnerable, disrupt communications and their unpredictability forces an ad hoc response. As 9/11, Hurricane Katrina and Virginia Tech all demonstrated, disasters often take unexpected, fast changing courses which forces responders and the public to improvise. None of the literature suggests that command and control is not necessary, but it does suggest we must establish flexible, innovative systems to gain situational awareness and partner with our public.

An article that appeared in the International Association of Emergency Managers Bulletin was written by Michael Byrne and Colin Whitmore, emergency management and homeland security professional from ICF International (an established emergency management and homeland security consultant agency). The article strongly suggested that homeland security officials must capitalize on the University of Colorado work by creating networked homeland security that addresses the aforementioned factors, utilizing increasingly networked mobile devices, involving users to capitalize on these devices' power through social networks, and incorporating "emergent behavior," which means groups are capable of higher collaborative thought and behavior than individuals (Byrne & Whitmore, 2008). This basically means that the whole is greater than a sum of its parts. The bottom line is that these elements could build a very robust system with many benefits.

However, the literature also points out these benefits do not come without potential problems. The first is loss of control by professional emergency responders, which could lead to a security risk that is unacceptable (Stephenson, 2007). Empowering the public to collect and relay information could lead to a mob behavior (Byrne & Whitmore, 2008). In addition, the public may view this system as a volunteer effort and now that membership in volunteer efforts such as Citizen Corps is dwindling, this may not be appealing (Council for Excellence in Government, 2004). Funding would also be

a problem, especially when the cost benefit ratio is so difficult to prove. As mentioned earlier, it is difficult to measure what impacts networked homeland security has, but the literature suggests it definitely has impact.

III. RESEARCH

A. GOAL

The goal of this research was to understand the various viewpoints of the value of Web 2.0. The literature review illustrated the potential benefits of this technology, especially the use of crisis informatics to capitalize on emergent behavior; however the researcher sought to understand why the tools are not readily accepted by the emergency response community. Much of the literature review concentrated on the public's use of social media, but little address the views of public safety officials. It is intended that the following methodology will help close that gap.

B. METHODOLOGY

The research component of this thesis is qualitative. It seeks to discover the attitude of public safety officials toward Web 2.0 and how existing social media can be used to engage the public in homeland security. The intent is to discover how social media is currently used, understand the value of networked systems, and provide a base of knowledge from which a model for implementation can be built.

First, the researcher conducted interviews with a variety of public safety officials. The goal was to target officials that had experience in more than one emergency discipline. Overall, this group tends to be the decision maker as to whether or not social media is to be utilized (see Figure 5). They can be the enabler or the obstacle. The interviews will help address how officials feel about the technology, their assumptions regarding public engagement and identifying barriers to implementation.

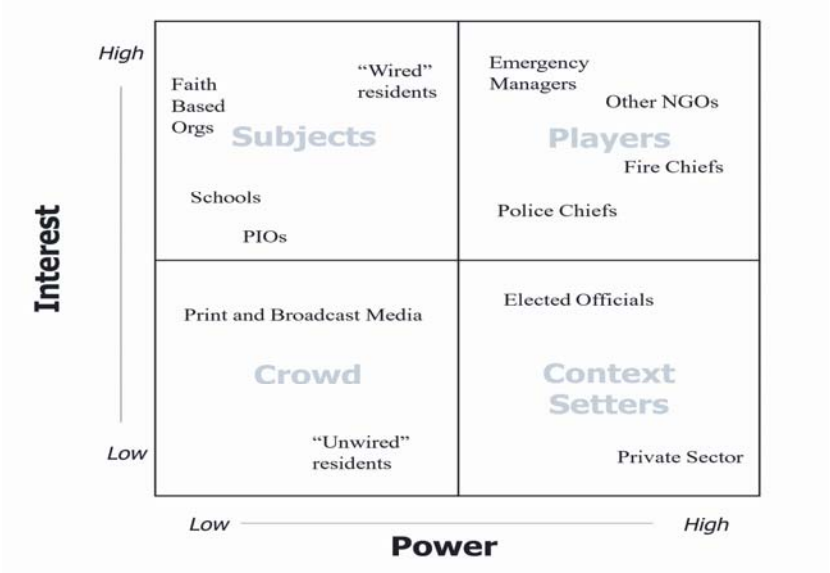


Figure 5. Interview Selection Tool – Power versus Interest Grid

The subjects were asked a total of 15 open-ended questions, which provided answers to the following categorical questions:

- *What gaps exist is current public information sharing models?*
- *Is there a role for the public in homeland security/emergency response?*
- *What is the professional emergency responder's attitude toward involving the public in response?*

The answers are complied in content analysis graphs at the beginning of each subsection, with supporting narrative included. The full list of interview questions and replies can be found in Appendix A.

Next, the researcher participated in "The OGMA Workshop: Exploring the Policy and Strategy Implications of Web 2.0 on the Practice of Homeland Security" help on June 30 and July 1, 2009 at the Naval Postgraduate School. This was an invitation-only workshop that consisted of Web 2.0 subject matter experts representing the categories of practitioners, behavioral science, network science and media, and technology. The opening sessions of the two-day event featured experts and leaders in the field of social media, highlighting work already done, work in progress, unanswered questions and their

view of social media's future. The subsequent breakout sessions were separated by the categories already mentioned and focused on the following questions:

- *What do we know and see in practice now?*
- *What requires further study, analysis and exploration?*
- *What are the requirements to achieve this?*
- *What partnerships need to be established?*
- *What collaborative bodies need to be formed?*
- *What funding sources are required?*
- *What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?*

The final component of this workshop was a report from each category to potentially map a way forward. The workshop was designed to be a candid, non-attributive discussion and debate about Web 2.0 and Homeland Security issues, so concepts will be addressed in this thesis, but will not be attributed to specific participants unless permission was granted. Coded notes from the workshop are included in Appendix B.

C. INTERVIEW ANALYSIS AND FINDINGS

Research participants were selected because of their level of expertise in multiple emergency response disciplines as well as those who have experienced recent events requiring enhanced communications with the public. While the sampling of interviews is limited in quantity, the perspectives provided are indicative of why leveraging social media is problematic for some organizations.

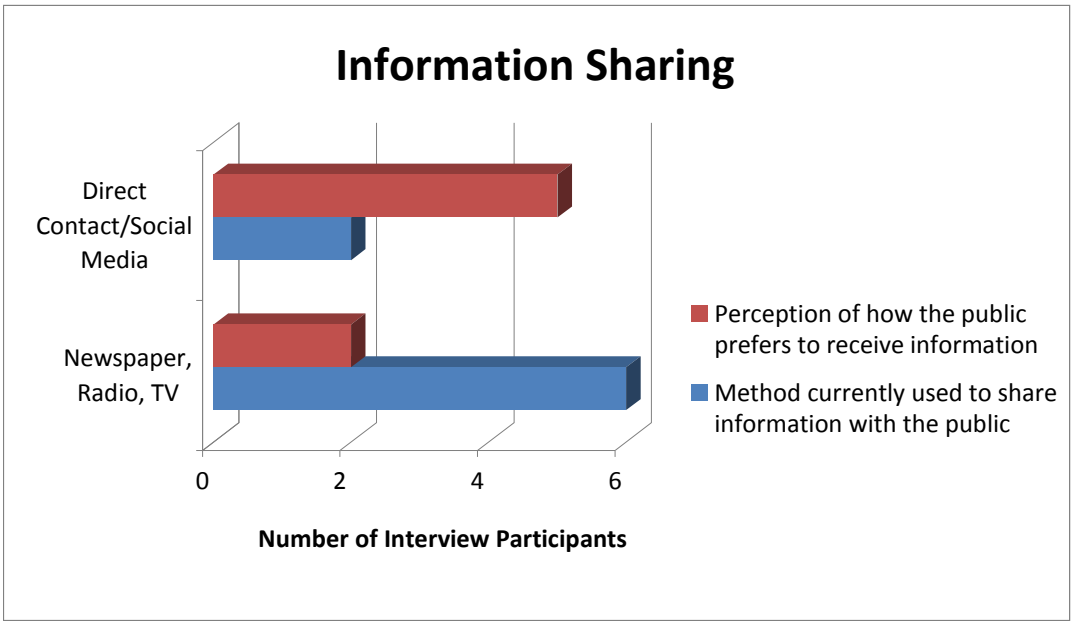
1. What Gaps Exist in Current Public Information Sharing Models?

Participants discussed how information is currently shared by their respective agencies and all referenced "traditional" means of communications. When asked to clarify, they mentioned the use of Public Information Officers (PIOs) to distribute

information to the media through direct interaction with media outlets or through a Joint Information Center. They also explained that the most commonly used mediums were television, radio and newspapers. Only two participants referenced the use of social media (specifically Twitter), text messaging and blogging.

The use these more "traditional" methods of communication appear to be in direct conflict with how the participants believed the public prefers to receive information. All but one said the public would prefer more direct, even person-to-person, contact. Tom Miner, program manager for one of FEMA's Urban Search and Rescue Task Forces, WATF1, commented on this disparity, "We keep using the standard press releases and news briefings and we target big media. Then we're frustrated that our message doesn't get out. The problem is the larger media outlets cannot deliver the community-specific messages that our citizens crave" (T. Miner, Interview, Washington Task Force One, 2009). He and other participants agreed that PIOs and JICs still need to be utilized, but there may be more tools (like social media) available for a more personal delivery of information.

Table 1. Information Sharing: Traditional versus Preferred Methods

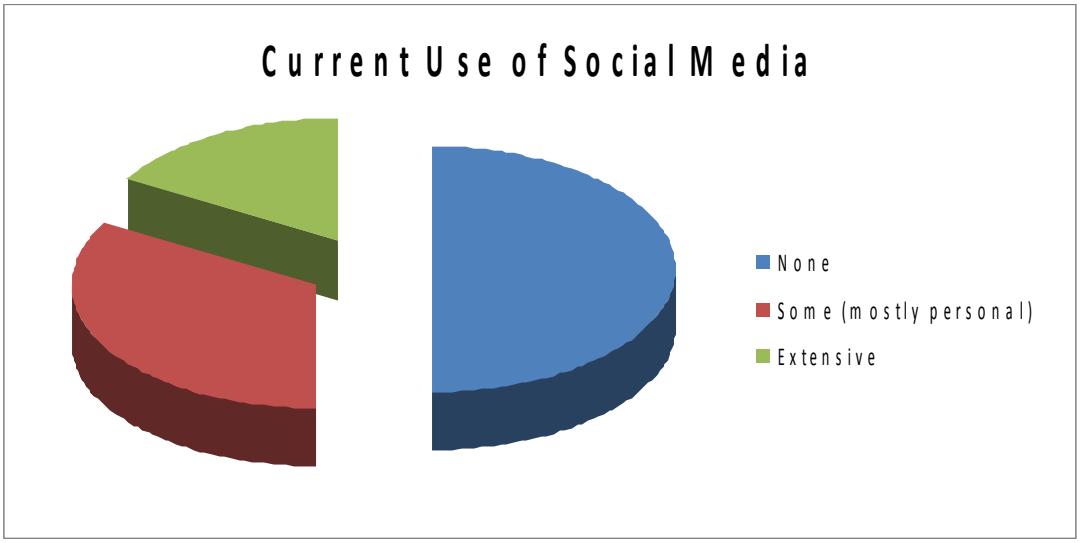


Miner went on to provide an example of what he considered an early version of social networking when his task force was deployed to Mississippi after Hurricane Katrina, "our team arrived and there was virtually no means of communication—there was no power, radios were not working well and cell phones worked sporadically. However, as we drove around the impacted community we dialed our radios into a small local station that provided us all the information we needed" (T. Miner, Interview, Washington Task Force One, 2008). This local radio station turned into a makeshift community information center where residents and business owners could provide the most up to date information. "Our team knew where we could buy gas, we knew what roads were open and most importantly, we knew who needed help and where they were located," said Miner (T. Miner, Interview, Washington Task Force One, 2008).

Next, it was important to understand why these traditional methods are still used when they may not be considered effective. Half of the participants had no experience with Web 2.0 tools. One interview subject (who chose not to be attributed), who has held leadership positions with local, state and federal emergency management agencies, noted his frustration with this topic, "All I know is that it [social media] is a huge pain. It is not convenient for me and there are just too many sites." This view and the lack of experience with social media are also referenced in the OGMA Workshop section to follow.

Two participants said this gap may be related to age. Specifically, they said that many public safety leaders represent a generation that is skeptical of, or rarely uses, technology, and this may prevent its acceptance. Pierce County Emergency Management Director Steve Bailey is cautionary regarding the use of social media because the messages may not reach those directly impacted by an incident. "Residents who are devastated by a flood are trying to make sense of what just happened to them—they're not on Twitter or Facebook," he said. "I do understand that social media is a tool in the toolbox, it just should not be the only tool" (S. Bailey, Interview, Pierce County Emergency Management, 2009). Two participants noted the use of social media in their personal lives, and they were now exploring its use professionally.

Table 2. Interview Participants' Use of Social Media



One participant uses these tools extensively. Port of Tacoma Security Director and professional blogger at www.disaster-zone.com Eric Holdeman points out that we must embrace social media because "we need to be where they are" (in reference to the public). "We must believe that people believe what they hear from peers —not what they hear from government or the media," he explained. "Just like 'nature will find its way' from the movie Jurassic Park, information will find a way—and we need to be participants" (E. Holdeman, Interview, Port of Tacoma, 2009).

2. Is There a Role for the Public in Homeland Security/Emergency Response?

All interview respondents agreed there is a role for the public in homeland security and emergency management. All commented specifically that they believe the public wants to help in some way. Only one participant offered his answer beyond the emergency response context, which was not expected because the question was specifically framed around response. Steve Bailey noted the important of engaging the public pre-disaster (S. Bailey, Interview, Pierce County Emergency Management, 2009), which will be identified as a way to address some of the trust issues identified later in this research.

Eric Holdeman said the public are the true first responders and "unlike some of my colleagues, I think there are strong roles for them to play" (E. Holdeman, Interview, Port of Tacoma, 2009). When asked why type of roles, he identified the more typical role for volunteers which includes sandbagging during floods, assisting with search and rescue and debris cleanup, as did other respondents. He did add, however, that the public could play a critical role in situational awareness, especially since a high percentage of the public carry cell phones. Holdeman argued that we are missing a great opportunity to engage the public as remote sensors in the community, continuous delivering real time information through social media. "I believe electronic relationships breed digital trust," he added (E. Holdeman, Interview, Port of Tacoma, 2009).

Sara Lepp, a volunteer center director in North Dakota, saw first-hand during the recent floods that the public wants to and can help. She coordinated the efforts of many hundreds of volunteers and social media played a very important part in that successful engagement. Lepp mentioned a concept related the public's role in emergencies that none of the other participants mentioned. Like the others, she agreed there is a role for the public and she believes they trust want to help. She also noted that individuals want to be the one to tell other people new information (S. Lepp, Interview, Firstlink Volunteer Center, 2009). This plays directly in to the concepts of sensors and networks where public safety officials can utilize members of the public to distribute and gather information. Greg Brunelle from the New York State Emergency Management Office said that officials should take advantage of the way the public self organizes to respond during emergencies. He said that faster, better information sharing through social media would better situational awareness and allow officials to make more effective decisions regarding resource allocation (G. Brunelle, Interview, New York State Emergency Management Office, 2009).

While all agreed there is a role for the public in homeland security and emergency management, they also agreed that any role must be part of an organized system. Here the participants were relating their answers to specific experiences with existing volunteer groups (search and rescue, sandbagging, etc.). Four were very specific that volunteers, in general, should be identified well in advance, trained, and their skills somehow built into

the emergency planning process. With the sample of participants, this is not a surprising development. Theirs is a centralized, command and control environment. The public tends to operate in a more network-centric environment.

3. What is the Professional Emergency Responder's Attitude Toward Involving the Public in Response?

In the previous section, interview respondents agreed there is a role for the public. The researcher wondered then, if they really trusted the public's reaction to emergencies and if they would utilize the public in all phases of emergency management—prevention, preparedness, response and recovery. When asked how they think the public reacts to crisis situations, all but one said that the public rarely panics. This was surprising because there seems to be a prevalent myth in the emergency response community that the public tends to panic. One interview participant said, "The public reacts calmly and in an organized fashion and the images we often see in the media are not representative of the whole." He did qualify his answer to note that we are probably witnessing fear rather than panic, which is consistent with findings in the literature review. Eric Holdeman said, "Research shows that, contrary to popular belief, people do not panic. Most people are willing to assist with their time, effort, money and other resources" (E. Holdeman, Interview, Port of Tacoma, 2009). That brought the researcher to the next questions regarding value and negative impact the public may bring to emergency response.

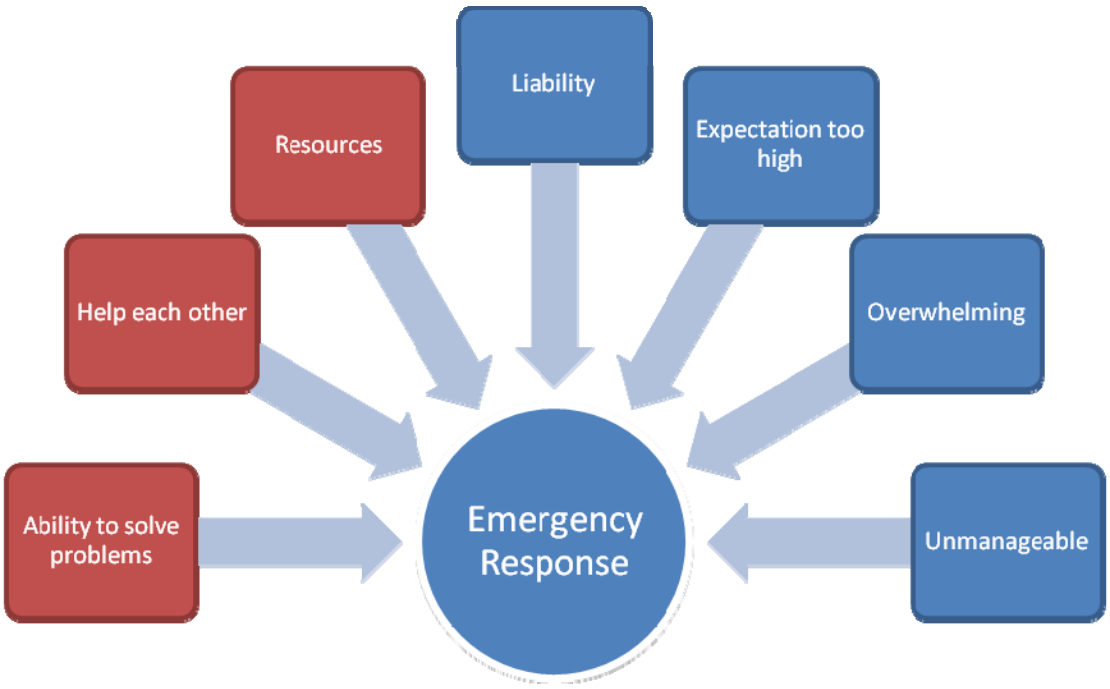


Figure 6. Positive and Negative Impacts of Public Participation During Emergencies.

.Half of the interview respondents claimed that the ability to solve problems was the most valuable quality the public bring to emergency response. On similar vein, two said the public's value is that people will help one another is times of crisis. "The public bring great value—expertise, resources and situational awareness," said Eric Holdeman, "Timeliness is also one of their greatest assets. Collectively, their resources, when motivated, can exceed that of public safety and government as a whole" (E. Holdeman, Interview, Port of Tacoma, 2009). Greg Brunelle from New York State Emergency Management agreed and said that in times of disaster there just are not enough responders and we need to engage the public to assist (G. Brunelle, Interview, New York State Emergency Management Office, 2009). Steve Bailey sees the public's strength in the ability to quickly assist one another because it will take some time for professional responders to arrive. "This is a relationship that must be developed," he added (S. Bailey, Interview, Pierce County Emergency Management, 2009).

With the positives, come several negatives, according to the interview pool. Half of the participants said that individuals who want to help can become overwhelming and

the situation can become a problem of its own. “We tend to encounter too many people that want to help,” said one participant, “this becomes more of a problem than a help. It can be overwhelming. I’ve had far too much experience with well meaning volunteers who want to run off and be heroes.” Steve Bailey said a negative impact could be related to expectations. In his view, the public does not react well to disaster because their expectations are too high. He added, “To compound that problem, we do not separate messages to those affected by disaster and the spectators so the communication is less effective to both groups” (S. Bailey, Interview, Pierce County Emergency Management, 2009). Two respondents view liability as a negative impact regarding the public’s involvement in emergency response. These participants shared the concern that social media would be a means for the public, well-meaning and not, to share misinformation and rumors. That combined with its apparent lack of organization makes it difficult to the public safety official to understand. The researcher believes this is why public safety officials are so insistent is folding the public into a command and control system. Sara Lepp provides the following example:

> *There needs to be a coordinated system in place to manage and place them. Volunteers can get hurt; they can also decide to sue. There needs to be liability coverage for issues that occur. They may not have the proper training for a situation. Volunteers should be screened according to what tasks they are doing and who they are working with. If a volunteer is working with vulnerable populations such as children or elderly, they should have a background check. The amount of people that respond can also cause traffic congestion and other problems.* (S. Lepp, Interview, Firstlink Volunteer Center, 2009).

During the interviews, it appeared that the participants had more negative than positive examples of engagement with the public. Unfortunately, they had all experienced this first-hand, with multiple events, across the nation. It is important to identify these issues to come up with a way to move forward. Steve Bailey was willing to see a middle ground (unsolicited by the researcher), “I do see that technology and social media could allow us to better communicate and build citizen infrastructure. I guess my only concern is that we’ve got to be careful of what we are asking for. If we ask the public to be

engaged and participate, we'd better be able to provide the mechanisms and support to handle that" (S. Bailey, Interview, Pierce County Emergency Management, 2009).

D. THE OGMA WORKSHOP: EXPLORING THE POLICY AND STRATEGY IMPLICATIONS OF WEB 2.0 ON THE PRACTICE OF HOMELAND SECURITY

On June 30 and July 1, 2009, the Center for Homeland Defense and Security (CHDS) at the Naval Postgraduate School, hosted an invitation-only workshop to discuss issues related to Web 2.0 and its application in the public safety arena. More than 80 participants attended, representing the following categories: Practitioners, behavioral science, network science and media and technology. The workshop included a brief introductory session followed by a series of breakout sessions that allowed each sector to share ideas and debate issues. It culminated with a report from each group outlining a possible path forward. OGMA was designed to be a non-attributive discussion of the following questions:

- *What do we know and see in practice now?*
- *What requires further study and analysis?*
- *What are the requirements to achieve this?*
- *What partnerships need to be established?*
- *What collaborative bodies need to be formed?*
- *What investments (time, personnel, funding) are required?*
- *What other types of resources are needed to advance our adoption, understanding and the utility of the new forms of communication?*

The researcher was asked to take notes throughout the workshop that would ultimately become part of a yet to be published report. Analysis of OGMA Workshop notes will aid in answering the primary research question of this thesis: *How can Web 2.0 technologies be used to formulate a model that will engage and create a role for residents in Homeland Security response?*

1. Overview of Web 2.0

Dr. David Boyd, from the Department of Homeland Security's Science and Technology Directorate, started the workshop by challenging the participants to think and lead differently. He said the primary goal should be to make information useful and actionable because "at the end of the day, it's the information that matters." Information must be identified and collected, managed and it must make sense. Then it must be shared and protected. Boyd explained that the information itself did not need to be protected, but the mechanism by which it is shared. Until now, the focus for interoperability has been radio communications. The desire is to expand grant programs to include other information technology. Boyd said the priority is to get information to people who need it in whatever form they need.

Chris Essid from the Department of Homeland Security's Office of Emergency Communications then offered the concept of citizen-centric communications that are open, free and widely used. One of the slides from his presentation said, "Web 2.0 provides a platform that enables citizens to self organize, share information, creating synergies that tap into the wisdom of crowds." He did note that these new technologies are an opportunity but recognized they do require staff and other resources to take advantage of them.

2. First Breakout Session

For the first breakout session, each group met separately. The notes from this session were voluminous and posed a challenge for analysis. To bring the key concepts forward from more than 11 pages of text, a world cloud was applied and produced the results in Figure 8.

Figure 7. OGMA Word Cloud

The world cloud clearly identifies information as a key issue. Similar to the comments offered by Dr. Boyd, the emphasis on information is greater than that of technology. Discussion ranged from what types of information need to be shared with the public, to how officials and responders get information from the public and how to deal with the assumed information overload that comes with the use of social media. The word public is also much larger than the word government in this analysis. Many of the conversations revolved around the fact that the public is the ultimate consumer of information and they need it to make potential life saving decisions.

Another group of words received nearly equal emphasis and capture the essence of why this workshop was conducted—need, use, better, social and tools. In fact, the assumption behind this thesis research is government needs to use better social networking tools to engage the public. Workshop participants wanted to better understand what tools are available and how they can best serve the public's need for information. On a related topic, the word Twitter also has particular emphasis because of this discussion. All groups made the point that Twitter was not the only Web 2.0 tool.

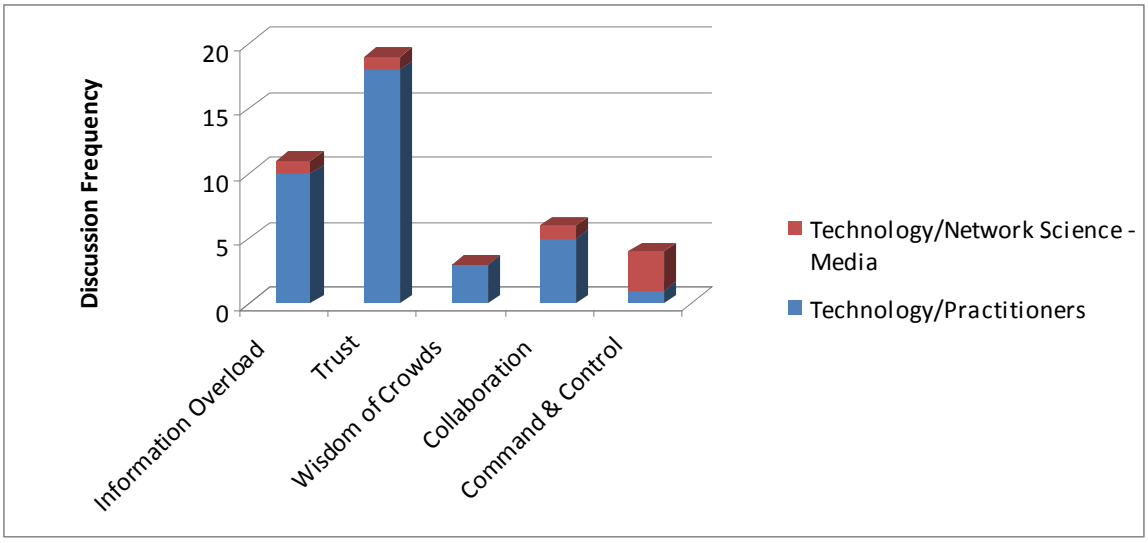
As the remaining analysis will show, trust became one of, if not the most important issue discussed at this workshop. However, the word trust received little emphasis in this initial breakout session.

3. Results of Round-Robin Sessions

a. Round-Robin #1

The first round-robin session paired the technology and practitioner groups and the behavior science and network science/media groups. The goal of these round-robin sessions was to bring new perspectives to the issues discussed within the original groups.

Table 3. Web 2.0 Primary Issues from Round-Robin #1



Information overload was a frequently discussed topic and is the greatest fear of practitioners. Many are reticent to utilize Web 2.0 technologies because there is no mechanism to sift through the volumes of information. For example, with thousands or even millions of Tweets coming in from Twitter, how can public safety officials analyze and evaluate the information and then organize the data to be valuable. One participant suggested that practitioners resist the urge to respond to every piece of information and simply look for trends and verify those trends.

In comparison to the initial breakout session, issues of trust were most frequently discussed. Again, practitioners seem to have the biggest issue with trust. With

every account of misinformation and misuse of social media was an example of how the technologies were used to stop rumors and deliver critical information. One practitioner said the social media networks could not be compared to trusted sources in a personal rolodex and a technology representative asked if one could really trust every person in the rolodex. They agreed to disagree. What the group did agree upon was the fact that relationships needed to be built to create trust.

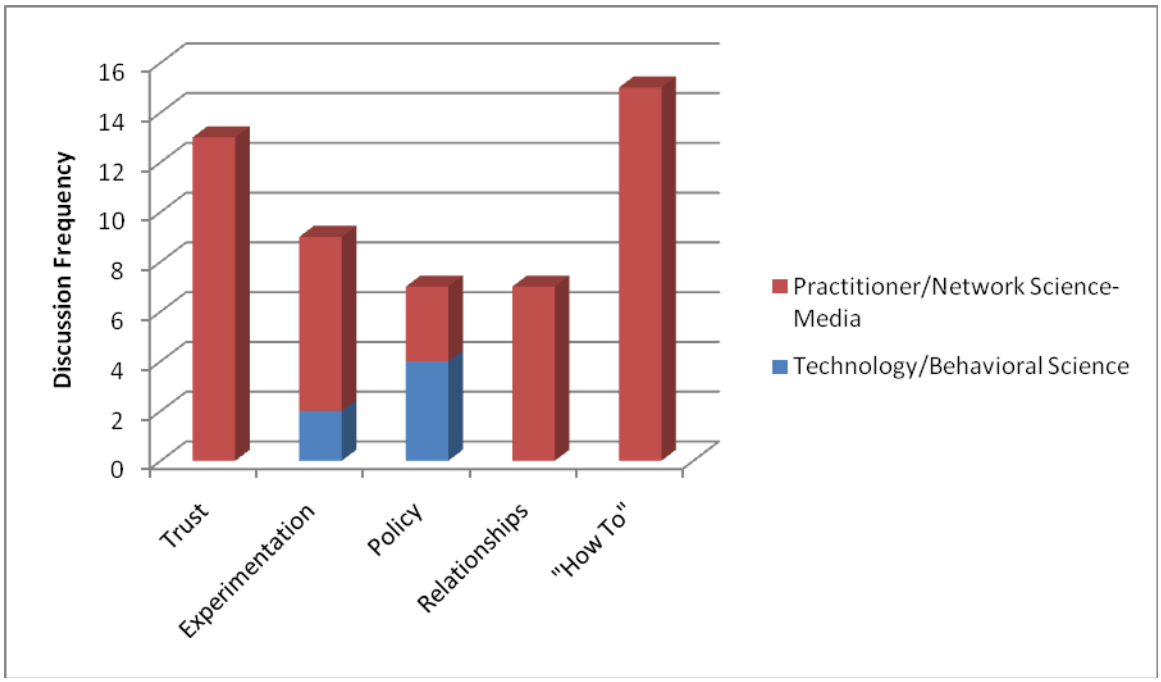
Building on the notion of creating relationships, collaboration was identified as a key discussion point. Workshop participants suggested partnerships between government and citizens, between multiple networks and systems, and between media, government, citizens and Emergency Operations Centers. The discussion lent itself to the discussion regarding wisdom of crowds. The technology group touted this concept while the practitioners remained skeptical.

Another key issue raised during this discussion was command and control. However, it was only mentioned once by the group containing practitioners, which is surprising because most operate in a command and control environment. The behavioral science and network science/media group asked if social networking and command and control could coexist. They concluded that Web 2.0 is not just social networking technology; it is about communicating across agencies and jurisdictions. One participant suggested a virtual command and control system that would pull in all partners. The group also discussed control in the context that government and public safety must resist the urge to control social media. They need to focus on being participants in the network.

b. Round-Robin #2

For this round-robin session, the technology group was paired with behavioral science and practitioners were paired with network science and media. While some discussions were similar to the first round robin, some new issues arose during this session as indicated in Table 4.

Table 4. Web 2.0 Primary Issues from Round-Robin #2



Like the first round-robin session, trust was a popular topic, but only among the practitioner and network science-media participants. The question remains, "how do we build trust." One suggestion was to trust but verify, meaning one cannot blindly accept everything. Another participant said that trust can be built because truth clusters and errors scatter, so users of social media can monitor traffic and key words through a variety of sites and systems. When the same chatter appears through multiple channels, resources can be sent to verify that information. The group was reminded that trust was not just an issue directed to public use of social technology and that practitioners must also strive to be trustworthy. As in the earlier session, it was noted that trust could be built by using Web 2.0 on a regular basis rather than just when emergencies unfold.

New to this session was the issue of experimentation and research. The groups agreed that more research needs to be done and to conduct the research, the tools must be used. The practitioner and network science-media groups agreed that best practices must be shared so that experimentation can be conducted. One participant said,

"We need to get familiar with the tools and be able to pick and choose which ones can be applied to different situations." To expand on the concept of experimentation, the same group identified the need to establish relationships. An OGMA participant noted that "different people need different structures to use and share information." Homeland security and emergency management communities need to partner with technology and network scientists to identify requirements and let the developers align systems to meet the need.

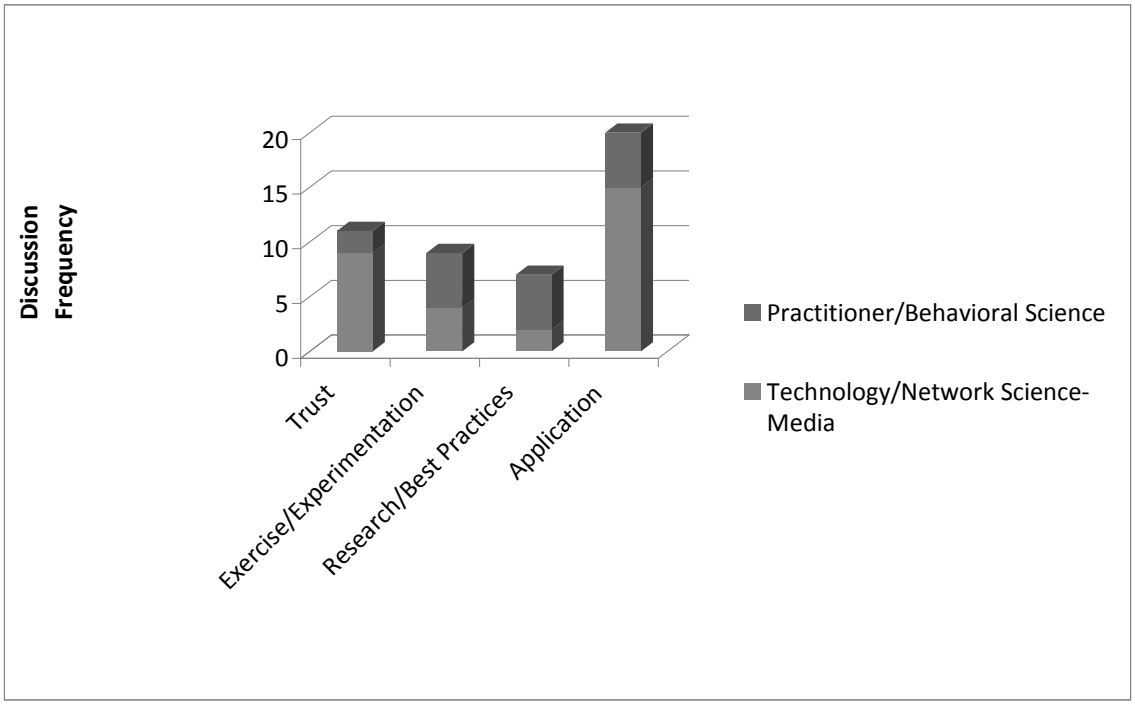
The two groups were split nearly even regarding their discussion of policy. The technology and behavioral science groups wondered why governmental agencies blocked the use of Twitter and other social media applications. They realized it was problematic to expect practitioners to use social networking when they are not allowed access. It was noted, in fact, that some agencies that block the use of this technology actually had established sites on Twitter, Facebook and MySpace. The discussion of policy was a bit different for the practitioner and network science-media group. The practitioners wanted some type direction or guidance from government regarding the use of social media. The group also noted that, based on their experience, it was very difficult for government to admit that current communication tools do not work. They are left with the problem that the worthiness of Web 2.0 is acknowledged, but 90 percent do not use it. The group wondered if the opportunities of social media could be more quickly harnessed with the support of policy makers.

The most popular topic of this session was the creation of a "how to" guide, but the discussion was limited to the group that included practitioners. This makes sense because this was the group least familiar with social networking tools. The practitioners suggested the development of guidelines, or a primer, on how to use social media effectively. One participant said that "if you expect me to embrace this topic, you'd better teach me how to use it effectively." Another participant noted that the practitioners are not the only ones who might need the "how to" guide. There should be a concerted effort to train social media users (the public) on the proper way to collect information and take photos, so they can provide actionable information to practitioners.

c. Round-Robin #3

The final round-robin session paid the technology and network science-media groups and practitioners with behavioral scientists. As these discussions continued, there were four primary topics—trust, exercise/experimentation, research/best practices and application of Web 2.0 technologies. The most popular by far was application. The researcher believes this is a direct result of the "how to" discussions from the previous session.

Table 5. Web 2.0 Primary Issues from Round-Robin #3



The trust discussions continued with a specific focus on the quality information. What became more apparent to the group was the need for experimentation and conducting exercises to determine the effectiveness of social media tools. Someone suggested the development of "communities of practice" to help guide the use of these technologies. These same "communities of practice" could become users of Web 2.0, which would enhance the level of trust among all participants. The groups felt this

experimentation should be paired with research, with the ultimate goal of sharing best practices. There are numerous examples of successful social media use, but there not mechanism to share that information.

The most discussed topic of this final round-robin session was application of Web 2.0 technology. Are there design principles and templates available? How much time and training do social media require? Do we need to invest in more infrastructure? Should social networking be handled through Joint Information Centers and Public Information Officers? How do we integrate social media into our Incident Command Systems? How do we reach our intended audiences? While the session produced more questions than answers, it set the stage for further work in this area.

4. Findings/Conclusions

To conclude this workshop, each participant group was asked to identify key issues, potential solutions, suggested players and a list of obstacles and enablers. A series of Venn diagrams will follow to show the level of agreement among the participants. All four groups agreed that strategy and policy were key Web 2.0 issues. Participants felt it was important to articulate the theory of this business and by defining the why, the how and what can then be determined. Issues of trust as well as adoption and implementation were considered key by three of the four groups. It is hoped that a trusted system can be developed to push information, pull information and mobilize resources.

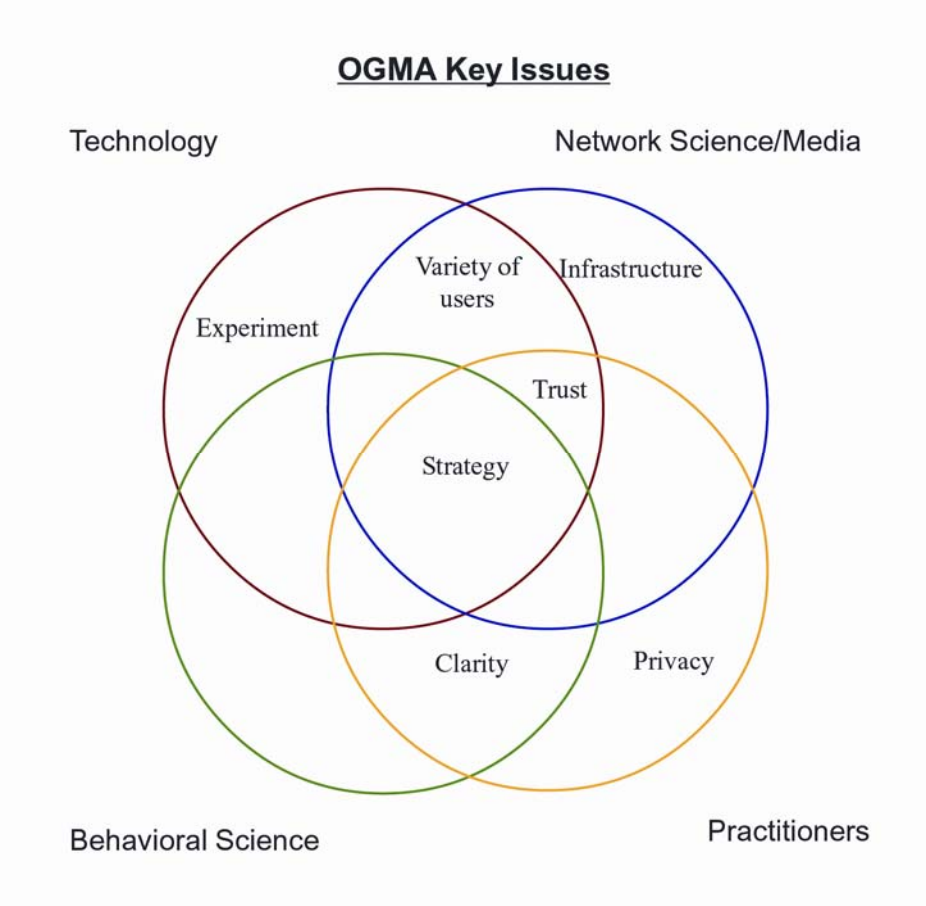


Figure 8. OGMA Key Issues – Final

The groups agreed that two potential solutions to this Web 2.0 issue are experimentation (combined with research) and education. Knowledge is important, so the group suggested pilots, test bed demonstrations, exercises, mandated use of Web 2.0 among own work teams, workshops and enhanced outreach. There must be a way to translate research into practice. Three of the four groups agreed that collaboration and the sharing of smart practices were potential solutions. "Sharing is critical," said one participant, "we need a clearinghouse of smart practices, communities of champions and cross pollination of practitioners and researchers."

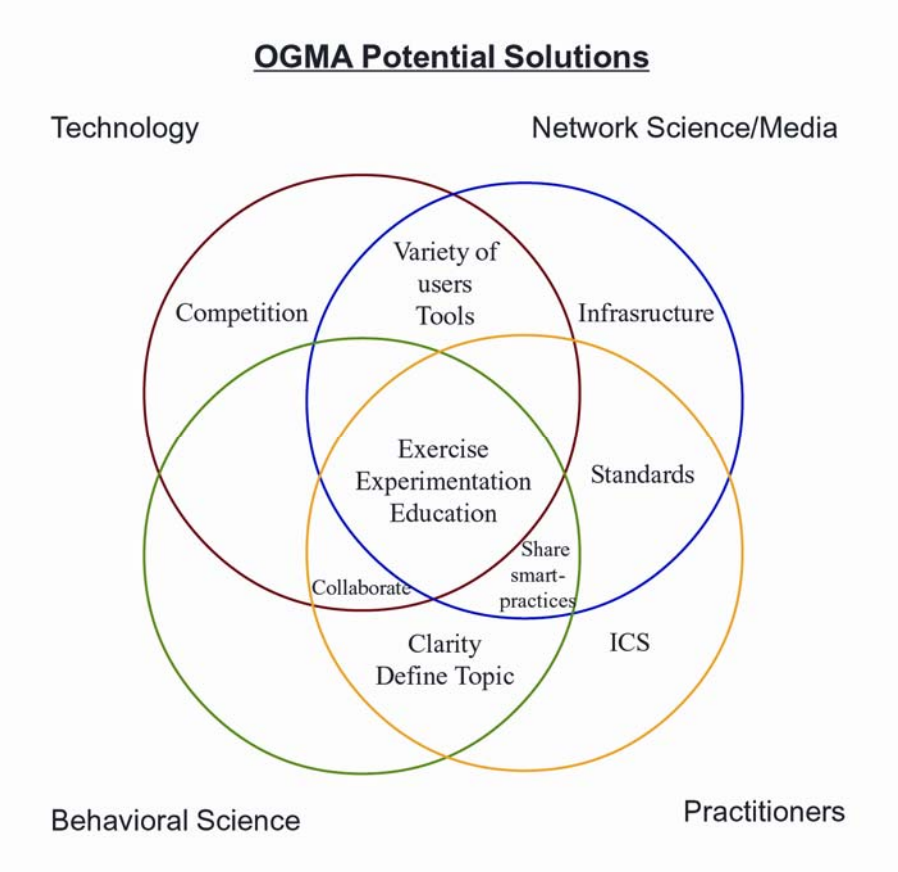


Figure 9. OGMA Potential Solutions – Final

The final topics were those of "obstacles" and "enablers" in the context of the use of Web 2.0. Unfortunately, the practitioner group did not offer a list, but the remaining groups agreed that funding was an issue. Some saw funding as an enabler because the technology is free while others saw funding as an obstacle because resources are required to utilize these free tools. The list of obstacles included awareness, security policies, fear of technology, culture and changing fads. Youth were considered enablers as well as research grants and engaged, passionate citizens. When it came to suggesting players or participants in the social media application to homeland security, all groups agreed the list should include public safety organizations, industry (private sector), and academia.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS AND CONCLUSIONS

A. SUMMARY

This thesis has reviewed literature, analyzed the thoughts and observations of a variety of stakeholders, through interviews and participation in a Web 2.0 workshop, regarding the use of social media to engage the public in homeland security and emergency management. The following sections will summarize the key findings and conclusions for each of those research efforts.

1. Literature Review

Social media connects people and helps build communities. It is not just a tool to disperse information (Drapeau & Wells, 2009). The goal is to engage and better interact with the public. Utilizing Web 2.0 is less about the technology and more about harnessing the power of emergent behavior because the public is not just a group of browsers and readers; it is a group of providers and participants. Unfortunately, government agencies are doing a poor job of using social media to engage the public (McCarty, 2008).

The current status of civic engagement can be best summarized in Bach and Kaufman's research where they site, "the American public has been left out and is largely missing in action" (2009, p.1). However, this phenomenon is not solely associated with homeland security and emergency management. Overall, civic engagement has been on the decline for the past 30 years (Putnam, 2000). One of the reasons for this social disconnectedness is the fact that government officials and the public fundamentally misunderstand and mistrust each other (Bach & Kaufman, 2009). This notion is consistent throughout the literature review, stakeholder interviews and the OGMA workshop. Public safety agencies spend a great deal of time getting to know one another, but that courtesy is not extended to the public. Asking individuals and families to create emergency kits does not equal civic engagement. Social media can help government

connect with the residents it serves. Tools for making friends in cyberspace have the potential to transform homeland security and emergency management in unexpected ways (McCarty, 2009).

Panic is often used as an excuse to discount the public and note engage them. Some officials even claim that information should not be shared because it may create panic and unruly behavior. Based on the literature, the opposite seems to be true. People tend to respond to crisis creatively and with collective resourcefulness (Ripley, 2008). If regular people get as panic-stricken as we think, one could assume that Flight 93 would have destroyed the White House or U.S. Capital. In the next section, the interview pool recognized the research that panic is rare, yet they still have issues trusting the public's crisis response capabilities.

There is strength in decentralized, starfish-like networks. While government operates in a centralized, hierarchical organization, the public does not. They tend to work through networks of strong and weak ties to share information and solve problems. This further explains public safety's resistance to embrace social media—it is a networked concept not well suited for a command and control world. Stephenson and Bonabeau (2007) are proponents of creating a networked homeland security system that capitalizes on social media and the use of personal communication devices. University of Colorado researcher provided examples from Virginia Tech and the California wildfires to demonstrate how these tools have been used to effectively seek and broker information, accurate information.

2. Interviews

Government uses traditional forms of communication (television, press releases) during emergencies even though they believe the public would prefer a different, more direct medium. This reinforces the conflict of a hierarchical versus networked organization. It is also problematic that public safety officials are not familiar with the social media tools utilized by the public. Some did note, however, that there was some

value in having social media as a tool in the toolbox, but not having it become the only tool. One interview respondent summed up his view in a simple phrase, “we need to be where they are” (E. Holdeman, interview, 2009).

Participants agreed there is a role for the public in emergency response, but it needs to be well organized and established pre-disaster, if possible. Some might assume this is more government versus public rhetoric, but the researcher believes there is value in this insight. To move forward with the use of social media, there needs to be some level of compromise. Public safety officials are uncomfortable with and may not trust random “tweets” from thousands of people they do not know or trust. Rather than discount this, maybe a more palatable structure can be created by applying social media tools onto a trusted network of volunteers such as amateur radio operators, search and rescue personnel or residents already involved in neighborhood preparedness groups.

Officials are also reluctant to engage the public through social media because the negatives appear to outweigh the positives. As noted in the literature review, there are liability, privacy and trust issues that must be addressed as social media becomes more prevalent.

3. OGMA Workshop

Bringing the public and public safety officials together through social media comes down to trust and the only way to develop that trust is to use the technology. Practitioners want to know how to use Web 2.0 tools so they are asking for a clearinghouse of smart practices and the development of a “how to” guide. Behavioral and network scientists want to conduct more research in the areas of homeland security and emergency management, but they have a limited pool of users to study. Ultimately, all parties want to learn more about the social media’s effectiveness and different types of usage, so experimentation plays a key role in moving this endeavor forward.

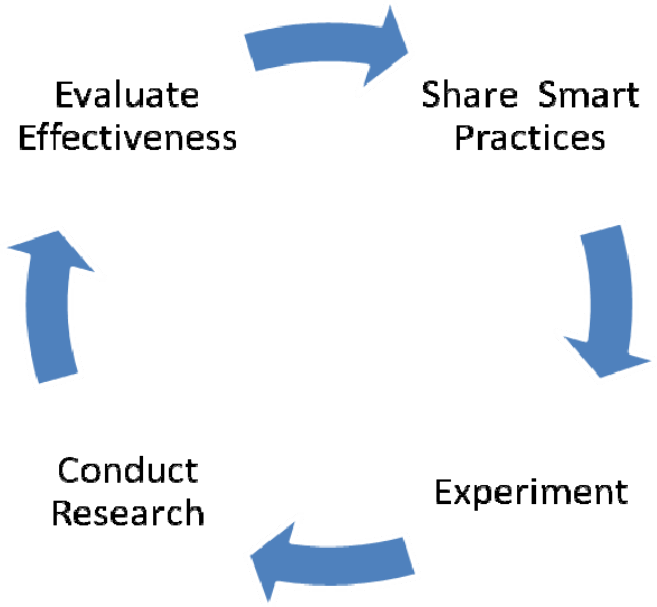


Figure 10. Public Safety Web 2.0 Cycle

B. PROPOSED MODEL FOR EXPERIMENTATION

The question is not whether to use social media to engage the public in homeland security, but rather how. The researcher wants to make it clear that other means of engagement, especially face-to-face interaction, should not be abandoned. Other methods can be enhanced by the application of Web 2.0 technologies. The research is clear that residents are using social media tools to seek and broker information and ultimately solve problems. Unfortunately, public safety has not been a partner in this endeavor and has missed a great opportunity to harness the collective power of the public. Individuals are capable of doing far more than preparing an emergency kit for the next disaster.

For the youth in our communities, social media is second nature. At the same time, the concept overwhelms those in public safety. The thought of sifting through thousands, even millions, of potentially irrelevant posts or "tweets" is enough to send officials running the opposite direction. For some, the only exposure to social media is the comment section following a news story in the on-line version of the local newspaper and this may not be representative of how people use social media pre, during or post disaster.

The researcher proposes a model in which social media is applied to an existing trusted network in the community. Most jurisdictions have a group or groups of trusted agents such as amateur radio operators, search and rescue volunteers, citizen corps representatives or neighborhood response networks. The focus should be to tap into the expertise of these existing groups to address the trust issues identified by public safety practitioners. The idea was brought forth during the OGMA workshop as was identified conceptually as a "Twitter Posse." While this would obviously include social media tools besides Twitter, the concept has merit. What is also important is working with this trusted network pre disaster, again to help establish the trust that practitioners and users alike will seek. Citizens want to know someone is listening and that government is providing accurate information, and the same can be said for public safety.

For example, the researcher is interested in linking more than 450 Pierce County Neighborhood Emergency Teams (PC-NET) in her home jurisdiction through a combination of tools or some sort of emergency management Wiki. It is not assumed that participants would know how to use these tools, so an education campaign would be launched to not only train people how to use social media but how to gather information and take photos or video that would provide actionable information to public safety officials.

To address prevention, the participants could use the wiki to share crime prevention tips, successful mitigation measures and suspicious activity reports that do not necessarily merit a call to 9-1-1. The information could be shared with the local intelligence group or fusion center. To address preparedness, the participants could blog about a specific topic (Van Leuven, 2009) or share smart practices regarding emergency kits, neighborhood trainings or upcoming exercises. It is assumed that the network would then use the wiki to share situational awareness and assist one another during disasters. This would also address the desired delivery of community-specific information that residents may not receive from the nearest media market. They would not only be points of information distribution, but also collection points for the community survey desperately needed by emergency responders. The wiki could also carry over into recovery, when neighbor helping neighbor is critical. Disaster assistance does not make

survivors whole; it simply gets them through the initial disaster. Using the wiki to identify unmet needs and match those with volunteer labor and resources will facilitate community recovery.

Working within a trusted, manageable network will be less intimidating to practitioners and would facilitate the research needed to measure its effectiveness. There are numerous Web 2.0 tools that can do many different things. The point is to find a tool or tools that meets the needs and fits the strategy of one's own organization. While it is important to experiment, it is more important to experiment with a strategy. Linking social media to known, trusted networks meets that end, creates trust and provides an arena for further research. There is value innovation (see Figure 11) in moving beyond the traditional means of engaging the public through brochures and mass media. With virtually no capital investment, public safety agencies can capitalize on tools used by the public every day.

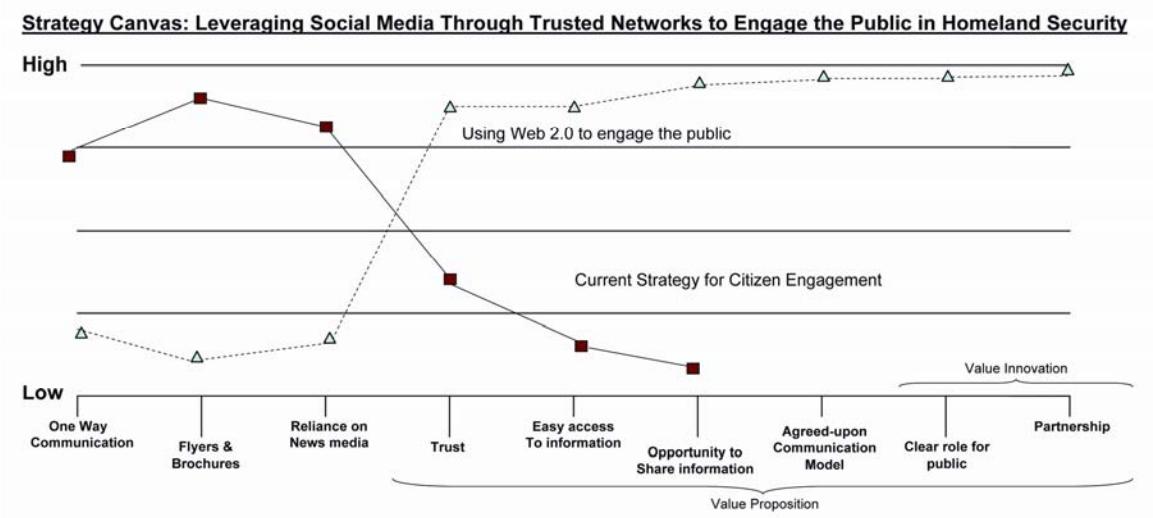


Figure 11. Value Innovation of Social Media

C. FUTURE RESEARCH

There is a great deal of opportunity in social media research. Some proposed topics are how social media and official government warnings compare during emergencies, how social media can most effectively direct the public to more complete warning messages and how the public utilizes social media as an emergency moves into an extended length of time—do their habits change? The world's current experience with H1N1 flu would provide a great laboratory to research how the public is using social media to prepare for, respond to and recover from a pandemic. There have been media reports that Twitter was inducing hysteria, but researchers did not observe the same phenomenon. A closer look at this scenario would be valuable,

Along with future research must come a collection of smart practices and ultimately the development of a "how to" guide for homeland security and emergency management officials. This should not only include how to use the various Web 2.0 tools, but also how to integrate social media into existing government public information systems. As stated earlier, it is important to recognize that this is not simply another way to push out information; it is a way to become part of a conversation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

A. INTERVIEW 1

Research Question	Interview Questions	Interview Reponses (BL)
What gaps exist is current public information sharing models?	1. Using a recent event as an example, how do you share emergency information with the public? 2. What factors contribute to successful information sharing with the public? 3. If you could build the perfect information sharing model, what would it consist of? 4. How do you think the public prefers to receive emergency information? 5. Please tell me what you know about or your experience with Web 2.0 technologies (wikis, blogs, social networking sites, text messaging, photo sharing site, etc.). 6. What gaps or barriers currently exist when it comes to sharing information with the public?	*Interviewed June 5, 2009* 1. It's not a recent event, but during the eruption of Mt. St. Helens in 1980, it was the first time a Joint Information Center was used. I worked for FEMA and there was no coordinated message – multiple reports of fatalities and each jurisdiction were saying something different. That is what became the store. The JIC/JIS system is still employed and still works 2. You must have a credible source and believable information. The key is saturating the media market with information. Just focusing on the five o'clock new doesn't cut it anymore. Social networks are very important. 3. I don't think there is a perfect model. 4. I think CNN is still the public's number one choice, televisions news is the most convenient way to get information. 5. All I know is that it is a huge pain. It is not convenient and there are just too many sites. The people who use this site don't seem to have many social skills. 6. I've tried using the technology and I just don't like it – I guess that is a barrier.
Is there a role for the public in homeland security/emergency response?	7. What plans/procedures does your agency have in place to utilize the public during an emergency? Do you accept text messages, photos, etc.?	7. There is a credibility factor when there is a 24 hour news hole. In the search for balance, reporters always look for an opposing opinion which can be problematic. How can the public actionable information,

	8. What role do YOU think the public would like to play during an emergency? *(I want them to make some assumptions here on behalf of the public)* 9. We've discussed what role you think the public wants to play; now what role do you think the public should play during an emergency? 10. What could individuals contribute to emergency response?	especially with instances like the H1N1 flu, when every piece of information is countered by another. More time needs to be invested in being credible. 8. I think the public wants to help but untrained volunteers can be a problem. There must be structure and discipline or responders will get overwhelmed. 9. People want to be safe and people want to help. 10. I think if people can get trained and get organized, they can help. I've had too much experience with well meaning volunteers who want to run off and be heroes.
What is the professional emergency responder's attitude toward involving the public in response?	11. Overall, how do you think the public reacts to crisis situations? (examples: terrorist attack, natural disaster, health crisis) 12. What value does the public bring to emergency response? 13. What could be the negative impact of involving the public in emergency response? 14. Over the past five years, has your agency changed how it involves the public? How so? 15. What incentives exist to involve the public? (answer as a responder first, then as a private citizen)	11. They help each other. 12. People don't panic and contrary to popular opinion, they do not loot. They do more than they're given credit for. 13. They need to get acquainted and have a plan. 14. I've discovered that the public can be a problem rather than a help. We just get too many people and it can be overwhelming. 15. Whether I like it or not, this is the world around us and the way people communicate. People are using it so I don't see that we have much choice.

B. INTERVIEW 2

Research Question	Interview Questions	Interview Reponses (SB)
What gaps exist is current public information sharing models?	1. Using a recent event as an example, how do you share emergency information with the public? 2. What factors contribute to successful information sharing with the public? 3. If you could build the perfect information sharing model, what would it consist of? 4. How do you think the public prefers to receive emergency information? 5. Please tell me what you know about or your experience with Web 2.0 technologies (wikis, blogs, social networking sites, text messaging, photo sharing site, etc.). 6. What gaps or barriers currently exist when it comes to sharing information with the public?	*Interviewed June 11, 2009* 1. Through the Emergency Operations Center and Joint Information Center. We share information through press releases, media interviews, press conferences, reverse 9-1-1, email, phone calls. 2. The problem is no one is very successful in this endeavor. We attempt to do it as many ways as we can. It seems like we're often providing information to those who aren't even directly impacted by the incident. We must reach those most impacted if we want them to see the "face of government: 3. We try to solve all of our problems through technology –we've certainly improved but it isn't the ultimate solution. During our recent floods, those directly impacted were not using technology and were not following the media. Those impacts do not get enough information. The answer is person to person contact which is the basis for many of our preparedness and recovery programs. 4. There is a high expectation that government will put them (disaster survivors) back or make them whole. I think they want to receive information face to face. Expectations will never be mitigated if we are not good listeners during disaster – they want to see us whether it is in the neighborhood or a community meeting. We need to have trained groups of people to reach out, assist and fill gaps. 5. None 6. The barrier is how social media seems to be used. I've heard about examples where untrue stories are

		getting sucked into the social networking vortex and are viewed as mainstream news.
Is there a role for the public in homeland security/emergency response?	7. What plans/procedures does your agency have in place to utilize the public during an emergency? Do you accept text messages, photos, etc.? 8. What role do YOU think the public would like to play during an emergency? *(I want them to make some assumptions here on behalf of the public)* 9. We've discussed what role you think the public wants to play; now what role do you think the public should play during an emergency? 10. What could individuals contribute to emergency response?	7. My agency focuses on direct communication. The problem is technology keeps expanding with no credible basis for understanding what it is we're trying to solve. 8. They want to be involved – view damage, report back. It's very important to invite the public to participate. 9. People who are not impacted want to view the disaster, critique government and comment in forums. This is of little value because they are just spectators. Others want to help by donating money and goods and by volunteering. Actual victims are so preoccupied that they have tunnel visions – you never really hear much from them. 10. The key is engaging the public before disaster strikes. This can be very difficult work, especially when you do not have regular incidents – it's tough to keep their interest. It also takes a lot of resources. I think there could be a role for spectators in technology – maybe we could funnel their energy into a usable arena.
What is the professional emergency responder's attitude toward involving the public in response?	11. Overall, how do you think the public reacts to crisis situations? (examples: terrorist attack, natural disaster, health crisis) 12. What value does the public bring to emergency response? 13. What could be the negative impact of involving the public in emergency response?	11. I believe the public will contribute by neighbor helping neighbor. The key is that relationships must be built – it's a matter of channeling them in the right direction. 12. The public does not react well because their expectations are so high. We are not separating messages to those affected and the spectators so the communication is less effective to both groups. 13. Many adults have issues with technology and may not know how to use it. 14. We've really come to an understanding that we cannot do it

	14. Over the past five years, has your agency changed how it involves the public? How so? 15. What incentives exist to involve the public? (answer as a responder first, then as a private citizen)	all. The power outage that left nearly all of western Washington in the dark a couple of years ago was a good example of that 15. I do see that technology could allow us to better communicate and build citizen infrastructure. I guess my only concern is that we've got to be careful of what we're asking for … if we ask them to be engaged and participate; we'd better be able to provide the mechanisms to handle that.

C. INTERVIEW 3

Research Question	Interview Questions	Interview Reponses (SL)
What gaps exist is current public information sharing models?	1. Using a recent event as an example, how do you share emergency information with the public? 2. What factors contribute to successful information sharing with the public?	*Interviewed July 23, 2009* 1. For the Red River Valley flood of 2009, we used many methods to communicate with the public. We used radio, TV, newspaper, open meetings, televised meetings, press conferences and social media. The event was very well publicized given the severity of it. 2. We had problems with misinformation being given to the public. The PIO needs to be constantly paying attention and needs to coordinate the messages with all groups involved. The televised meetings held for the flood were very helpful for the public to not only receive accurate information, but to see the community leaders relaxed and calm. This meeting was watched by many people. Social media such as facebook, twitter and text messaging helped also to send updated information to people quickly. When people were sandbagging they weren't by the radio or TV, but they usually had their phone with them to see

	3. If you could build the perfect information sharing model, what would it consist of? 4. How do you think the public prefers to receive emergency information? 5. Please tell me what you know about or your experience with Web 2.0 technologies (wikis, blogs, social networking sites, text messaging, photo sharing site, etc.). 6. What gaps or barriers currently exist when it comes to sharing information with the public?	facebook of receive a text message. These tools worked really well to deliver messages quickly and effectively, especially to the younger populations. Many younger people do not read newspapers or watch the news often, but they check their facebook accounts many times a day. 3. Having one person in charge of all information coming in and out would help deliver one consistent message. The news and radio personnel need to focus on publishing correct information instead of trying to deliver the most shocking story to boost ratings. Agencies assisting with the situation need to coordinate their messages. Public officials need to go through the system as well, instead of saying off the cuff remarks that could be perceived negatively. 4. I think it depends on their age. The younger generation and even up to the baby boomer generation are on the internet and social networking web sites. The older population seems to prefer TV, radio or newspaper. People like instant gratification and aren't as patient as they used to be so any method that is fast and easy. I also feel that many people still watch the evening news as well as listen to the radio in their car. 5. I know how to use facebook and text messaging. I have not done blogs, wikis or twitter but know the concepts and how they work. 6. These technologies work great for information sharing. Information reaches people quickly through these tools and more people are using these tools than ever before. These technologies are very popular now and seem to be peoples' preferred method of sharing information. Posting and retrieving

		information from these tools is fast, easy and enjoyable.
Is there a role for the public in homeland security/emergency response?	7. What plans/procedures does your agency have in place to utilize the public during an emergency? Do you accept text messages, photos, etc.? 8. What role do YOU think the public would like to play during an emergency? *(I want them to make some assumptions here on behalf of the public)* 9. We've discussed what role you think the public wants to play; now what role do you think the public should play during an emergency? 10. What could individuals contribute to emergency response?	7. When you are dealing with a disaster or other emergency situation, information changes so rapidly. It's hard to keep up with the changes and involve all of the necessary parties. The public panics and then rumors are started. 8. We work through the City and County plans, which is to utilize a public information officer. We do not accept text messages or photos but do send out text messages. We can also post photos on Facebook as well as allow the public to post them if appropriate. The police department does accept text messages in the form of crime tips. If there was a situation when this made sense to do this, we would. 9. I think people like to know what is going on, especially during an emergency. They want to be involved and informed. They like to be the one to tell other people new information. They want to know if their home, family or friends are at risk. They also want to help in any way they are able. 10. They should stay calm, be prepared, stay informed and help when asked. They should obey the warnings and advisories given by community leaders. They should listen to and follow instructions regarding evacuations, volunteering, etc.
What is the professional emergency responder's attitude toward involving the public in response?	11. Overall, how do you think the public reacts to crisis situations? (examples: terrorist attack, natural disaster, health crisis) 12. What value does the public bring to emergency response?	11. I feel that most people do pretty well during these situations. However, this largely depends on the loss and disruption they experience. If they experience loss or tragedy, they don't do as well after the situations. After the attention and support goes away, they tend to suffer more. 12. The public is often the first to call 9-1-1 during car accidents and other emergency situations. They often stop to assist the victims as well.

	13. What could be the negative impact of involving the public in emergency response? 14. Over the past five years, has your agency changed how it involves the public? How so? 15. What incentives exist to involve the public? (answer as a responder first, then as a private citizen)	They may also perform CPR of first aid if they've been trained. They can also assist with whatever tasks need to be done. 13. There needs to be a coordinated system in place to manage and place them. Volunteers can get hurt; they can also decide to sue. There needs to be liability coverage for issues that occur. They may not have the proper training for a situation. Volunteers should be screened according to what tasks they are doing and who they are working with. If a volunteer is working with vulnerable populations such as children or elderly, they should have a background check. The amount of people that respond can also cause traffic congestion and other problems. 14. We have started using social media tools and have put more energy and thought into our web site. We have realigned where we spend our limited marketing budget based on the technology and information trend changes. We send out much more information over email and send much less through the mail. We also do many more activities over email and Internet than we have in past years. 15. n/a

D. INTERVIEW 4

Research Question	Interview Questions	Interview Reponses (TM)
What gaps exist is current public information sharing models?	1. Using a recent event as an example, how do you share emergency information with the public?	*Interviewed August 5, 2009* 1. We keep using the standard news briefing and press releases and we target big media. We're frustrated that our message doesn't get out, but we never send anything directly to specific communities. The traditional way doesn't work. We need to target

	2. What factors contribute to successful information sharing with the public? 3. If you could build the perfect information sharing model, what would it consist of? 4. How do you think the public prefers to receive emergency information? 5. Please tell me what you know about or your experience with Web 2.0 technologies (wikis, blogs, social networking sites, text messaging, photo sharing site, etc.).	people through reader boards, flyers, local small radio stations. During a US&R deployment to Mississippi, the only situational awareness the task force received was through a very small radio station that was basically transformed into a community message center. It was ironic that this station was excluded from large press briefings because there was no room. By listening to this stations, we had all the intel we needed – what roads were open, what gas stations were functioning and who needed help. 2. Identifying a target audience and figure out the message by looking at the situation. You have to recognize when you're not reaching those who really need the information. Need to capitalize on decentralized networks that are good at sharing information. We shouldn't forget about the media, but utilize these networks as well. We do have to be careful with social media because there is just too much information coming in – need to weed through the superfluous. 3. Can't disregard the media, but the planning function is any response will benefit from the information gathered through social networks. We must explain the information sharing process. We must monitor and listen – there is not excuse when the public says "I've been telling you this." 4. They want to hear from officials personally, not through a media outlet that is too large to meet their information needs. The people in Mississippi were so upset with MSNBC because they had no clue about their situation. The public prefers direct contact. If nobody explains the process, you're just setting up a situation of frustration. Must educate the public on how information will be delivering to and sought from the public. 5. Has some personal experience with blogs (recent vacation), but has not

	6. What gaps or barriers currently exist when it comes to sharing information with the public?	used professionally. I'm old and just can't keep up with these technologies but I can see how they would be a force multiplier. 6. The sharing of video and photos is most valuable. So many people just are not good at describing a situation or person. A picture is worth a thousand words.
Is there a role for the public in homeland security/emergency response?	7. What plans/procedures does your agency have in place to utilize the public during an emergency? Do you accept text messages, photos, etc.? 8. What role do YOU think the public would like to play during an emergency? *(I want them to make some assumptions here on behalf of the public)* 9. We've discussed what role you think the public wants to play; now what role do you think the public should play during an emergency? 10. What could individuals contribute to emergency response?	7. They have the capability to help and want to help. They just need to be folded into the planning process. The key for all parties is the sharing of real time information. 8. If people are not victims, they want to help. It makes people feel good to know they've contributed. Many want to donate, which is a problem because the items are often unusable. Others want to do things, but there is often no role for them to play. Involvement must be organized and coordinated. 9. The public has a lot to contribute and technology can be used to manage that. I see it as a great way to mobilize folks to assist. I can visualize social media strike teams that will share information with others as well as provide information to emergency officials. 10. included above
What is the professional emergency responder's attitude toward involving the public in response?	11. Overall, how do you think the public reacts to crisis situations? (examples: terrorist attack, natural disaster, health crisis) 12. What value does the public bring to emergency response? 13. What could be the negative impact of involving the public in emergency response?	11. They don't panic and they can have a role. If the public is actively engaged, professional responders can focus on immediate life safety issues and then restoration of critical infrastructure. 12. The majority of people just do what they need to do to solve problems. With the proper education and understanding, they can simplify our lives. 13. They can become unmanageable and will become angry if they volunteer and are not utilized.

	14. Over the past five years, has your agency changed how it involves the public? How so? 15. What incentives exist to involve the public? (answer as a responder first, then as a private citizen)	14. We've had pockets of improvement. In general we're still teaching the public not to worry and that government will take care of it. We bail out businesses, tell people not to worry and tell them to go shopping. We're still missing out on the collective power of personal responsibility. 15. n/a

E. INTERVIEW 5

Research Question	Interview Questions	Interview Reponses (EH)
What gaps exist is current public information sharing models?	1. Using a recent event as an example, how do you share emergency information with the public? 2. What factors contribute to successful information sharing with the public? 3. If you could build the perfect information sharing model, what would it consist of? 4. How do you think the public prefers to receive emergency information? 5. Please tell me what you know about or your experience with Web 2.0 technologies (wikis, blogs, social networking sites, text messaging, photo sharing site, etc.).	*Interviewed June 1, 2009* 1. Through more traditional means – newspaper, radio, public education, etc. Once government web site became established, started posting information and eventually blogging. Twitter was not available or popular at the time 2. Transparency – not holding back any information. Doing such is just feeding the public half truths. We have to be cognizant of the right messages – three days of preparedness is not enough! 3. I don't think there is a perfect model or a perfect system. The key is a multi system approach – redundancy. People need to read, here, see and possibly experience the message (key is multiple means). The point is that we have "To be where they are." 4. n/a 5. I've had quite a journey through the technological world. I think emergency management does a better job of using technology and sharing information than most other disciplines. About 5 years ago, I started building an email contact list

	6. What gaps or barriers currently exist when it comes to sharing information with the public?	– when information needed to go out, it went via email. Once the techie folks said I could do this on the internet the blogging really began. About 18 months ago I started Twittering and now have 7,100 contacts. The only drawback is that I was cloned on Facebook! 6. Time, money and interest – actually the web takes money out of the equation. We must realize that people believe what they hear from peers – not from government or the media. We must go where they are. For too long, we've been happy to not be engaged – we just send out a press release and hope somebody bites. Now we can publish the story ourselves. A good example is Triangle of Life – it's a bunch of garbage that is passed around over and over again. Like "nature will find its way" from Jurassic Park, information will also find a way. During a recent widespread power outage, the power provider's website was visited the most when the most were out of power – it found a way. Another gap is the fact that we don't utilize the public as "remote sensors" – 80% of Americans have cell phones.
Is there a role for the public in homeland security/emergency response?	7. What plans/procedures does your agency have in place to utilize the public during an emergency? Do you accept text messages, photos, etc.? 8. What role do YOU think the public would like to play during an emergency? *(I want them to make some assumptions here on behalf of the public)*	7. None currently. My organization does not allow any use of social networking sites and hopes to establish a policy very soon 8. I think the public wants to help – not because we're asking them to. They're just willing to pitch in.

	9. We've discussed what role you think the public wants to play; now what role do you think the public should play during an emergency? 10. What could individuals contribute to emergency response?	9. Unlike some of my colleagues, I think there are strong roles for the public to play. The public truly is the first responders. As I mentioned, I consider them remote sensors that can deliver me very important information. 10. Resources and situational awareness. I believe electronic relationships breed digital trust.
What is the professional emergency responder's attitude toward involving the public in response?	11. Overall, how do you think the public reacts to crisis situations? (examples: terrorist attack, natural disaster, health crisis) 12. What value does the public bring to emergency response? 13. What could be the negative impact of involving the public in emergency response? 14. Over the past five years, has your agency changed how it involves the public? How so? 15. What incentives exist to involve the public? (answer as a responder first, then as a private citizen)	11. Research has shown that, contrary to popular believe, people do not panic. Most people are willing to assist (time, efforts, money, and other resources). Delivering more information will allow the public to make more effective decisions. 12. The public brings great value – expertise, resources, and situational awareness. People with out information will draw their own conclusions and act as they deem appropriate. Timeliness is also a great asset of an engaged public. Collectively their resources, when motivated, exceed that of government and public safety 13. Them getting the wrong message or not wanting to get involved. 14. n/a 15. Resiliency! It cannot be achieved without engaging the public

F. INTERVIEW 6

Research Question	Interview Questions	Interview Reponses (GB)
What gaps exist is current public information sharing models?	1. Using a recent event as an example, how do you share emergency information with the public? 2. What factors contribute to successful information sharing with the public? 3. If you could build the perfect information sharing model, what would it consist of? 4. How do you think the public prefers to receive emergency information? 5. Please tell me what you know about or your experience with Web 2.0 technologies (wikis, blogs, social networking sites, text messaging, photo sharing site, etc.). 6. What gaps or barriers currently exist when it comes to sharing information with the public?	*Interviewed August 6, 2009* 1. NYS uses the NY-ALERT (http://www.nyalert.gov/) system to communicate alerts and warnings with the public. We use the media via our Public Affairs office (ESF 15) as well. Recent examples of NY ALERT activations and PIO activities include the recent severe thunderstorms that resulted in wind damage and flooding in the lower Hudson Valley; the ice storm of December 2008 in the Capital Region; and the Continental Air Disaster in Clarence, NY on 14 February 2009. 2. Timely and thorough delivery coupled with the solid relationships we have developed with county and local emergency managers who are closer to our customers and, therefore, better able to gauge the effectiveness of message delivery. 3. Incorporation of 2-way messaging via the use of web 2.0 technology into NY-ALERT (developing). Additionally, it would be ideal to utilize a call center to gather data from responders and the community in near real-time. Developing NY-ALERT web 2.0 tools currently but we should explore using the state's existing call center (Tax & Finance). 4. Multi-modal to ensure delivery but the 'best' method is as direct as possible (face-to-face for the most affected from responders). 5. Extensive personal use and am currently incorporating FLICKR, Facebook and Twitter into our operations. 6. Most of our disasters result in telcom & power failures so technology is unavailable. We also

		have very limited staff to incorporate this new technology.
Is there a role for the public in homeland security/emergency response?	7. What plans/procedures does your agency have in place to utilize the public during an emergency? Do you accept text messages, photos, etc.? 8. What role do YOU think the public would like to play during an emergency? *(I want them to make some assumptions here on behalf of the public)* 9. We've discussed what role you think the public wants to play; now what role do you think the public should play during an emergency? 10. What could individuals contribute to emergency response?	7. Working that up this year. 8. Real-time reporting of needs (more efficient and targeted delivery of relief commodities) and better situational awareness. 9. same 10. Individuals already contribute – they self-organize and begin response/recovery ops. This can be augmented with faster, better information sharing.
What is the professional emergency responder's attitude toward involving the public in response?	11. Overall, how do you think the public reacts to crisis situations? (examples: terrorist attack, natural disaster, health crisis) 12. What value does the public bring to emergency response? 13. What could be the negative impact of involving the public in emergency response? 14. Over the past five years, has your agency changed how it involves the public? How so?	11. Calmly and in an organized fashion. The images of stranded persons at the Superdome in NOLA are not reflected a vast majority of the people affected by Katrina or peoples' reaction to disaster situations. 12. Very – in a true disaster there aren't enough responders. Citizens effort most rescues and initial response/recovery efforts. 13. Liability perhaps, if government gave advice that proved to be wrong and resulted in injury/death however this cannot serve as a block to information sharing. 14. n/a

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

A. OGMA NOTES FROM INITIAL BREAKOUT SESSION

Technology

What partnerships need to be established?

- University, startups, government grants. Ad hoc experiments.
- Capture best practices.

What collaborative bodies need to be formed?

- Exercises
- Strong Angel
- Golden Phoenix
- Cyber Storm
- California - Regional/State-Wide Exercises. Golden Guardian Exercise.
- Five year exercise plan in California
- Group can put forward exercise recommendations.
- Exercise must affirm some point of view.
- TOPOFF (Top Officials Exercise)
- No money and no time for full blown exercise. Get away from expensive, high profile, and useless exercise where no one fails.
- Academia (No)
- Private Enterprise
- Developers

What funding sources are required?

- State and Federal government has to assume the financial risk. Chief of Police cannot afford political or fiscal failure. Allow virtual participation in these experiments.
- What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?

Raw Data from Individual Break Out Session on Technology:

Any government organization is going to have a Web 2.0 challenge

- Framework - Detect, Protect, Respond, and Recover
- Architectural approach as opposes to a tool approach.
- Organizational Process
- How do we think about what we think?
- IT is changing the role of governance and creating new patterns of engagement.

- Participatory management and government.
- How do we build trust?
- Outward Sharing and Inward Sharing Framework?
- Is it the use of Web 2.0 that defines behavior or does behavior define Web 2.0?
- Established institution for Emergency Management in communications. Institution is coming to terms with Web 2.0.
- What can you do to stop the flow of information in Web 2.0?
- Sea of information. Some is garbage and some are silver dollars. Tweets may be gold or garbage.
- Ratio of trash to gold.
- Can you mandate it? Clayton Christiansen (Harvard) Disrupting Class
- You can't mandate the use of Twitter for a Fire Department.
- Government should not be in the business of developing social networking tools.
- Government had little to do with the development of the internet.
- The problem with every conversation that he has had with innovation in social networking. Don't create a gov twitter
- Organic systems that emerge in the context of the open web should not be reinvented.
- Google, Twitter, etc. can't deal with Privacy Act information.
- Can't ignore the aspects of law that limit sharing of certain types of information that the government possesses.
- Can't assume that law applies to all - most laws written to constrain government.
- Privacy rules do not apply in the private world as they do in the federal government.
- It depends on why you are twittering
- Within an organization, there are people allowed to speak on behalf of the organization or not.
- Government has twitter and has FaceBook pages.
- Gov should showcase best practices.
- Collaborative document workspaces - Microsoft SharePoint - is that Web 2.0?
- FaceBook and Twitter are part of the same ecosystem.
- Fail safe (Cold War) vs Safe fail (Today) modes?
- Protect data repositories

Summary - What's out there?

- Twitter
- FaceBook
- Google Earth
- Mashups (multiple technologies)
- Current Issues
- Adoption of technology

- Telephone
- PC
- Mobile Phone
- Internet (Web 1.0???)
- Internet/Mobile 3G (Web 2.0)
- Law's will be driven by the use of technology.

What should the Federal Government do?

- Leadership role?
- Maybe
- Government employees use Web 2.0 at home, but the same employees don't leverage technology in the workplace.
- The adoption issue is huge - three years ago to get law enforcement information pushed out to a law enforcement officers cell. Out of 1,800 L.E. Officers maybe only 40 use the technology.
- Fed does not push - it develops working circles upon working circles - this builds the kind of clout that you need. Fed does not get to be in charge.
- Fed should state the end-goal - local, state, and private sector will reach the target/goal.
- Fed should publish best practices
- Open source world - Government provides the opportunity.
- Internet's strength is decentralization.

What is Web 3.0?

- Web 2.0 euphoria - "we" are all rushing in.
- If Twitter goes down then someone will create a new site.
- Government should come up with models of coproduction. Incubate technology.
- Academic - 3 degrees of influence - new book sociologist.
- Top issues
- Technology Adoption
- Innovation
- think about issue differently
- experiment (how the government funds research - $3.4 Trillion R&D) only $50M for law enforcement. Lack of funding hurts co-production models.
- Think differently
- Experiment
- How do you form partnerships and then experiment?
- Combine the small pockets into a collaborative organization.
- Government funds and facilitates partnerships.
- Where and how do you experiment?
- What is critical infrastructure?
- How do you protect data repositories?

Are Twitter and FaceBook part of the critical infrastructure?

- Twitter does not consider themselves to be part of the critical infrastructure for the United States.
- You can't depend on cell phones. Power grid is going to go out. Fail safe mode is that first responders and incident leaders can execute their mission in a decentralized environment with sparse information. New technologies will not change the world during an emergency phase. Once emergency occurs - ALL BETS ARE OFF.

People are going to use the technology available to them every day. Information Quality Issue What is the accuracy? What is the value?

Key Issues raised during your sessions

- Adoption of Tech: Some parts of the public sector are reluctant to adopt Web 2.0 applications in their daily life. FaceBook – 200M; MySpace – 70M; Twitter – about 20M. Social networks may not be the best platform for emergency response situations. They should not be excluded, but these technologies cannot be relied upon exclusively.
- Innovation
- Experimentation
- Failure need to be alright in order to innovate.
- Start with small projects and build
- Learn from prior to disasters where tech has been adopted in an ad hoc way.
- You have to think about how you deal with issue differently in order to get on path to experimentation.
- The technology sector is best at solving problems, yet few problems have been posed by other working groups. Here are a few problems that came to light:
- Too much information inbound to single responder through Web 2.0 Apps.
- Aggregators
- Numerous Web 2.0 Apps (Facebook, MySpace, Qik, Wikipedia, etc.)
- Is there one portal or platform that can manage these disparate forms of input?
- Authentication
- Data Assurance
- Portable Identity
- Standards Compliance
- Interoperability at high-level.
- Information Quality
- What can the tech sector do to ensure that quality or verification exists.

Web 2.0 Apps that did not get mentioned:

- Collaborative
- Ning
- Wikipedia
- Intllipedia

- Base Camp
- KoHo
- Huddle (UK)

Potential methods for finding solutions to each issue

- Exercises?
- Let's see where the current system breaks and then fix it with available and inexpensive technology available.
- Experimentation
- Co-production
- Competition to develop useful applications
- Apps for democracy example
- Give developers the problem and then let folks solve it.
- Annual prize for needed solutions

Raise the issue to the following orgs:
Build Awareness
Media
Government (Federal, State, Local, Tribal, etc.)
Industry Group
No industry group so you have to target individual companies.
Public safety organizations
Target groups that can get things done
Money
Players/organizations who should be involved in working the solution
Same as above group
"Obstacles" & "Enablers" currently in place to hinder/facilitate a solution

Obstacles

- Adoption
- Awareness
- Security Policies
- Fear of technology and accessiblity
- Inconsistent Web 2.0 guidance from government
- Changing fads
- Gaps for underprivileged (Accessibility) Lack of inclusivity. Subsidize.
- Need champions to push this along (tech capable)
- Politics
- We need to know what we are trying to do
- Requirements in public safety community do not always work
- Sometimes end users do not know capabilities that exist
- How do you show the responder what is possible so that they can define their needs.
- You need to get to "Robust Statement of Needs"

Enablers

- New Generation (The Millennials) are “growing up online.”
- Politics
- Mechanism for confluence of interest
- Engaged and passionate citizens
- Need money

Practitioners

What do we know and see in practice now?

- Example of Monterey fires - witnessed the community self organized. Stood up blogs and web sites and were much quicker than govt PIOs
- People didn't think they were at risk - and it turned out they were right.
- New Orleans - neighborhoods used social media after the incident to post photos and share stories. They trust local law and fire more than media.
- H1N1 DHS is using social media to monitor what the public is saying about issues. Looked at RTs. There was a lot of fear and speculation. CDC was getting some messages out, but the RTs were disputing the official word like backlash.
- Inauguration postings that went out from DC were wrong, then the public corrected us and we listened and RT the correction. That's how we build trust. That's how we gained credibility.
- DC train crash - first hand reports were coming in too rapidly. EMs and broadcast media were receiving flood of reports. Needed to determine how many details to share.
- Media got information on the phone from official source that conflicted with that from citizen reporters.
- We need to give the public guidance.
- It is a two-way conversation. We need incorporate it for what it is. Don't try to change it. We use it for situational awareness, warnings and instructions. Understand the limitations of what you have - redundancies are inevitable. It needs to be conversational / casual.
- Received a streaming video of a kid with a gun to his head. We tracked it down (via Twitter?) It ended up being a prank, but we did act on it. This is relevant because if you don't do anything, you're damned. If you over react, you're damned. We need to take baby steps to investigate.
- Search and rescue missions will be helped by photos and context to help make resource allocation decisions.
- surfire.org as an example

Challenges

- Have to pay attention to other local, state messages
- Have to use all methods possible to disseminate the information
- Huge disconnect in recognizing that the public has better situational awareness than emergency responders.
- Have to restore the relationship with the public - explain the mentality of why (evacuation), why it took longer to share information.

- Do not agree that it is self-policing. Twitter messages are too fast to self correct, then recipients might not receive the RT
- We are just sitting on the sidelines while there is a big crowd / parting in the city (i.e. social media). We need to get involved.
- We are in the competitive environment where people are racing to get information out first. We have the mindset that we cannot do that. We need to be able to say this is what we know and then go back and correct it if necessary.
- Can't keep up with it. Need to be a participant. Need to provide verifiable information. If your source is from the public, then state that.
- Too much information!!!
- Information overload...If I have to add web monitoring, text messages, etc. I cannot resource it effectively.
- Knowledge and intelligence is aobut questions not answers.
- We can't be as irresponsible as the media
- If it's not about saving lives - I don't care.
- Need to engage with the public on their terms. That's why you should care. Politics from public pressure make a difference.
- I still need to know how to evaluate the data about when to respond.
- Privacy is a huge issue. Can only store it for 24 hours. Drill down if you see something happening, but must take it in aggregate. DO NOT STORE the information when monitoring it. (A Word to the wise!)
- I need accurate information - reliable. I cannot burn resources on a rumor.
- There’s no 911 twitter feed.
- But we might be able to have a national system of hashtag of 911 that places it into a different category that streams directly to a DOC.
- Need to be able to reach people in a geographical area with warnings and evacuations.

What requires further study, analysis, and exploration?

- How can I use social media to save lives. Reaction time is the most critical. I don't want to follow the nuts. It could create more problems to chase after false reports.
- Need to let go of the command and control mentality.
- How can we develop a system to sort out the bad reports from the valuable information.
- We have to think differently.
- Develop protocols for privacy issues of login information, names, etc. Blogs have less liability.
- How do we fill gaps in getting information out to the public?

What are the requirements to achieve this?

- Trust is key
- Every instance of warnings build trust after confirmation of incident specific
- Trust is not the only factor - the reinforcement of the message will override issues of credibility. (Mileti from morning session). People will choose to select the reality they want to.
- Must have a public alert system
- Must have a public affairs system - but it is also an operational tool.

- Need to train agencies on social networking.
- Recognize that this is a tool in the toolbox. State EOC need to synthesize the main points of what is being said.
- We have to clarify the goals of what we need from social media.
- Cannot argue and rally against this. We need to use younger people to help guide us. We need to engage in the conversation and learn about it.
- Need the geographic ability to notify public.
- If the media can deal with these independent citizen reports, then Emergency management community needs to master it too. We shouldn't be that far behind getting information out.

What partnerships need to be established?

- It's the gov'ts role to aggregate all the social media reports for the public. If the gov't doesn't do it the media news outlets will.
- Need to involve the survivors.
- Create staffing opportunities in other jurisdictions / agencies to share the resource drain.
- How should we engage with CERT or NERT, volunteers?

Network Science/Media

What do we know and see in practice now?

- Seeing better and better data, finely tuned, from the field. Better tools – Google Earth, databases, etc. During operations, very difficult to get a common operating picture – law enforcement had different terms for the same things. Texas – volunteers on horseback had much better situational awareness. Created system for multiple individuals agencies to feed information into Joint Operations Info Center – fed info back out to all participants.
- Coast Guard Citizen Action Network – utilize people with deep local knowledge to feed information to those who need it.
- Trust is a big issue – information coming from known groups vs. general public.
- Issue is often a never communicated with B. What we need is a fully distributed system because disasters do not know boundaries. Must be a way to become an instant member of this network. This is not a high security situation – must be inclusive. There must be a way to involve the public before an event happens.
- Mass convergence – everybody shows up. It's very common yet people are shocked this happens. It is difficult to manage this. How can agencies use social media to help shape this process?
- We are seeing self organizing groups use the media to enhance their work. Rimoftheworld.org – 20 year olds with existing social networks used social media to share information during CA wildfires (San Bernadino). Professional responders used this group to gain situational awareness. Concern about a common threat. Authority rested on the information. Self correcting information. Flexible, dynamic, transparent
- Institutionally organized – groups working together. There is another thread – incidental information (no organized group). This is info coming from someone on their blackberry or pda.

- New Zealand – focus is on citizen participation. Building a culture of preparedness – plan, respond, recover (donations). Emergency management is lead but relies on residents.
- Information overload is an issue.
- You can pull, push and mobilize through social media. People should be cautious to only focus on the first two. Mobilization may be one of the key issues.
- Distributed knowledge among the public – most have tools to help share this information.
- Reaching the younger generation is not a problem – it's pulling information from them or from their networks.
- Wikimapia – citizens participating in community database. This is an example of something citizens can use on a daily basis.
- Virtual Alabama, Virtual Louisiana
- Microsoft Vine

What requires further study, analysis, and exploration?

- How can we replicate the CA wildfire example in areas that experience a variety of hazards? They shared a set of skills and had a common goal. We need to determine where the investment comes from.
- Can we distinguish between organized groups and individuals using social media?
- Is there a way to leverage this information that is being captured by professional media outlets? Monitor websites, blogs, etc. – open source intelligence.
- Can social media be used to help manage emergency volunteers?
- Should we establish ground rules for use of social media? There has been evidence of a conflict between fire PIOs and citizen reporters (San Diego). Who has the "official" information?
- How do we capture information from all these various communication tools?
- Develop/enhance systems to engage the community.
- Using social media to mobilize people during an emergency.
- How can we develop a framework to organize social media information into actionable categories.
- How do you maintain a level of trust? Can we develop a common doctrine?
- Automating information synthesis
- Scalability

What are the requirements to achieve this?

- We need to constantly experiment – will our culture allow this?
- The future of social media – Twitter may be very different in 10 years. It might be better to capitalize on existing technology rather that creating something new. How can you better leverage current users to share information for you?
- The ability to demonstrate value. Measurable outcomes.
- Local ground-truthing
- Can security levels be established? Certain audiences would have access to different levels of information. Have there been any security breaches (individual, business, DoD, etc.)

- We need to capture and share smart practices

What partnerships need to be established?

- Communities of practice. Sign on to discuss smart practices (formalized milling)
- Establish authorized Tweeters in communities
- Government and private sector (analyze if that partnership can always be trusted).
- Partnership with locals – keep them engaged and information consistently updated.
- Partnership with public – train them how to collect information (maybe media can provide the training

What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?

- Need better tools. Find a way to avoid information overload.
- Need to use tools that people use every day (if it's not used regularly, it is likely to not work).
- We should be cautionary about rolling everything into one package. Each tool may do something different and reach a different audience.
- Wikimapia – citizens contributing to database
- Training
- Provide locals with a better ability to participate
- Policies may need to be changed

Principles
Provide locals with better ability to participate
One size does not fit all
Obstacles
Scalability
Policy Change
Information Overload
Liability/Paranoid
Pace of change
Usability
Ability to adopt organizationally
Media now relies on citizen reports – often uses social media rather than sending a reporter to the scene. It provides them the opportunity to continue to be "first."

B. CODED OGMA NOTES FROM FIRST ROUND ROBIN

Technology-Practitioner

What do we know and see in practice now?

- Concerns about information overload
- But: When do we not get overwhelmed? We always have to respond and react to it.
- Example of the DC metro crash. Conflicting information reports. Once verified, sent out a tweet with the information that the station was closed. That resulted in building trust and followers.
- San Francisco 311 – has requirements for non-emergency messages (twitter) requires some type of collected reporting protocols. Illustrates a trust-building atmosphere within social networking environment that will benefit in the future.
- Social media helps communities take care of themselves. It also may help us with resource allocation decisions.

What Challenges exist?

- Volume of information and emergent data is intentional and signifies an urgent situation.
- Practitioners have this grip and grin approach. Mental rolodex of how things are accomplished – past very anecdotal in how response is implemented.
- Social networks can also develop trustworthiness – this point was disputed. No, it is ever-changing and you can't compare it to the rolodex strategy of trusted sources.
- How do you balance the function versus the

- How do you measure trust? [great question; maybe info science has something to offer about this -- e.g., http://bit.ly/8tBFp] What do you trust? We trust the accuracy of information from historical sources.
- How do we organize data to be valuable? It needs to be analyzed and evaluated.
- Wisdom of crowds is valuable, but how do we trust it? Does volume = truth?
- Example of Twitter on the Iran elections – it did not give an accurate portrayal of what rural Iranians were feeling – it was skewed to by the masses.
- Have to trust it. We always here this complaint from EMs.
- Maybe we should allocate resources to disprove the wisdom of the crowds, rather than dismiss it out of hand.
- Fear of deliberate attempt to disrupt. Just because we fear it doesn't mean it will be happen. It does mean we have an increased risk.
- By not participating, we are making a mistake. The next big disaster will involve independent citizen reporters.
- The fact is that some bloggers and twitter users have built trust over time and have a community of followers – more so than emergency managers. Example of local gov't fewer followers than tech savvy individuals.
- Need to recognize that people who engage with online communities are connectors to a wider audience.
- Why can't we just call 911? The problem is that it may not contain the same information. A Tweet may have different information.
- Next generation of 911 will include text messages.
- We can prosecute violators of 911. Too many other tools diminish resources that have been placed on driving people to 911.
- Web 2.0 is not just Twitter!
- How do we harness it to be predictive?

What requires further study, analysis, and exploration?

- Twitter is not the only resource. Not all tweets will reach the audience. We can aggregate tweets in a way that places value on the overwhelming topical trends. This data will help evaluate the validity of an event.
- Is there a wire diagram? Where does EM fit in this new emergency world of information via social networking?
- We need to be able to filter the information. What methods could be used to verify the information?
- Sometimes the rolodex provides inaccurate information.
- Need to have a system for verifying data before we can mobilize resources.
- Wisdom of the crowds – touted by Technology group. Not accepted by some practitioners.
- The nature of the analysis has to change. Develop trust of the sources, then you have a trusted source.

- Is the issue about what is real or what is social pressure of what the "perceived truth" is? The social construction is real.
- EOCs stream TV reports – but they pull from many of the same sources as the internet. What's the difference?
- New sources can compute and provide analysis. Can you build perpetual computing mechanisms to provide that verifiable checklist?
- Need to have gov't involved to prescribe how we are going to use it and then roll it out to the public. There is great public value to getting it right.

What are the requirements to achieve this?

- Need to aggregate the tweets and see a trend – wisdom of the crowds can be valuable in the context of large volumes of data.
- Follow the numbers rather that the one individual report that may not be accurate. Look into crowdsourcing.
- Need to have two-way information sharing. Need to invite the public to contribute.
- But the public has no skin in the game. I have to make quick decisions and allocate resources. I'm responsible for good decisions.
- Need software to filter the data and identify trends.
- If we rely on Twitter, must make sure the tweets involve the right data.
- This is not a zero sum gain. This is an evolution. We need to get on top of it.
- Need to develop a system solution.

What partnerships need to be established?

- Develop relationships or history and trust with social network sources.
- Some institutional trust can be valuable. The online community has trusted sources.
- Need to develop partnerships between media, citizen reporters and EOCs.
- Twitter posse – layer of autonomy away from EM structure but close relationship.
- Develop guidelines of how to do community based social networking collaboration from public to engage with EMs and other impacted public. Volunteers? Standards?
- Use this regularly during non-emergencies. Build up a comfort level.
- Build trust by using day to day social networking for crime statistics – provide information that is valuable for the public.
- The reporter is trying to be helpful.

What collaborative bodies need to be formed?

- Partner with other "trusted sources"

What funding sources are required?

- The expectations for how information will be shared are going to impact new investments in the future.

What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?
Outcomes?
Strive for valuable applications every day to build trust and community with followers.
Interoperability is at the center of this.
We need to show value added for the players involved.
There aren't any silver bullets.
Need to experiment with it.

Behavioral Science/Network Science and Media

What are you hoping to get out of this session? Steal good ideas. Control, security, privacy – can be dependent on type of disaster. Application of media across all phases of emergency management – not just response. Maximize local knowledge in any threat environment and translate that into actionable information. Communicate with all partners. Public safety to public safety communication. How do we address the changing nature of technology. How can we control misinformation. Twitter streams – is there a way to analyze how that network emerged and determine level of truth. Social media impact on/implications for law enforcement. Wants to see agencies get permission to use these free tools. Harness these tools to do something for someone. Use these applications to deliver warnings to those who may not receive them via other means. Make connections to coordinate research projects. Make sure people can find the resources they need more easily. Networked vs. hierarchical means of communication.

Remaining Questions

- Security? Can we have technological systems to address all hazards that can also maintain a level of security? Good question for practitioner group. The private sector can set some standards and if standards aren't met, the level of trust will not be established with that participant.
- How do roles change over time? A good emergency system should have roles built in. Software doesn't always address that effectively. Web 2.0 is not a role base organization – everyone can be a player and that's the beauty of the system. We need to be participants and not try to control the system.
- Can social networking and command/control coexist? Maybe they can coexist without being the same system. See as big challenge when including public safety, military and public – we need to find a way to work together.
- Validity of information? Many systems already exist to ground truth information – "word cloud" can categorize information to make it usable for responders and weed out the irrelevant. The more we try to control the systems, the less people will participate.
- How does the media sort through citizen journalism? Engaging subject matter experts is best way to sort through information. Media does not exist as we once knew it and they do not sort through information – they do not have research staff any longer, nor the experience to vet the citizen contributions. They simply repeat it. It's not necessarily about accuracy – a story might be corroborated and it might not.

- Web 2.0 is not just the social network technology. It's about communicating across agencies and across jurisdictions – there needs to be a virtual command and control system that pulls in all the partners. Do we need a better definition?
- If social networking ceased to exist would it have an impact on your organization? Mixed response from group. It seems we're always trying to catch up with technology. Do we have to assume some level of risk?
- This is less about technology and more about creating social knowledge. We need to appreciate the range and rate of change in this environment. Information and knowledge about risk better serves all participants. Raising the level of understanding and increase the capacity of a community to manage its own risk.

Future Research? What needs to be done and who needs to do it?

We need to involve citizens in the planning phase – get them involved before response is necessary. Is it possible to show the benefit of doing so?

- Can a correlation be made between the benefit of investment in mitigation (investment of $1 equals saving $4) and an investment in social media? Maybe a similar strategy could be employed. How do we measure success?
- Who? Academia, practitioners – need better communication between the two. Practitioners need to know that academics are not reporters. Research is handled much differently – protection of human subjects.
- Emergency preparedness audits – may be necessary to show progress and to address shortcomings. Could be a way to move society forward.
- What do we know and see in practice now?
- What requires further study, analysis, and exploration?
- What are the requirements to achieve this?
  What partnerships need to be established?
- What collaborative bodies need to be formed?
- What funding sources are required?
- What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?

Key:	Information Overload 10/1 Trust 18/1 Wisdom of Crowds 3/0 Collaboration 5/1 Command & Control 1/3

C. CODED OGMA NOTES FROM SECOND ROUND ROBIN

Technology-Behavioral Science

1. What structures, resources, and actions need to be done?
2. Behavioral and Social Science Group meets the Technology Group

3. Capability: Aggregate data, analyze information, distribute information to business clients in order to create better marketing strategies. Web 2.0 information can be aggregated in order to support federal, state, and local needs.
4. Tech sector needs requirements in order to provide a solution.
5. Bob Josefek works with companies to understand virtual networks and social groups.
6. How do you frame the problem space to discuss virtual collaborative networks?
7. Homeland Security Blog: http://www.thehomelandsecurityblog.com/
8. Questions

Key Workshop Questions

- What do we know and see in practice now?
- What requires further study, analysis, and exploration?
- What are the requirements to achieve this?
- What partnerships need to be established?
- What collaborative bodies need to be formed?
- What investments (time, personnel, funding) are required?
- What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?
- Why do some agencies block Twitter?
- Often times it is because some employees are some unproductive. Many Government Agencies don't see the value in social networking. Integration of technology into organizations. If you don't control the message by assimilating technology then someone else will control the message for you. Communications people recognize that the organization needs to control the message. You have to be patient with the government with respect to adopting technology. One of the reason practioners react negatively to social science research is because they often don't find value in the research. Typically the finding is what is the next research step and how much funding do I need. BigMedicine # ogma Everyone has a story. Either you create your own story or someone else will craft one for you. Need a meaningful W2.0 story for all. Social scientist need to publish in practioner's journals. How do practioners get researcher to do relevant research? How do we expect to get social network sites into government when we can't even use IM or VOIP in this process?
- This is a "wicked problem"
- These modes of communication exist, growing, and will likely become a Tsunami. One day government will come along. Collaborative models of emergency management will give you better outcomes. Why not conduct an experiment? Let's create some experiments. Collaborative planning will give you better outcomes. Researchers want more info on how twitter, facebook are really being used. lots of anecdotal evidence, not enough info to conclude. How does government enable through new technologies for community resilience to emerge? The discussion re role of govt & sociotechnical models in building community reslience I think ought to be front & center #ogma RT @debbryant: government rep wants research data to be relevant and shared to practitioners in the journals the practitioners read. #ogma RT @ilabra discussion about role of

government and sociotechnical models in building community resilience ought to be front and center #ogma

Practitioner – Network Science and Media

What do we know and see in practice now?

- California Wildfires
- Texas border security
- Where can we see practices in place. What are concrete examples that we can study?

What Challenges exist?

- Human nature may trump the systems that people don't fully trust. In other words, if people decide that we will not follow the systems (monitoring of social media) we have misallocated resources.
- Can't use the excuse that we shouldn't use a tool because the bad guys can use it. It means we HAVE to use it and be better at it then they are.
- Even if we build a system, the public may not come. But crises will spawn more followership.
- Counterpoint: You have to have a system in place, which can be a resource drain.
- Heuristic concept – fear that allocating resources ineffectively may cost lives. Responders need to trust the source to deploy resources.

What requires further study, analysis, and exploration?

- How do we build trust? How do we engender trust in systems?
- How to demonstrate the value?
- Collaboration, cooperation and coordination are different things. Which areas do social media demonstrate value. If we work with trusted resources, we may not need to spend so many resources to verify. Coordination is where we plan together. Collaboration is where we work on the same problem. Bring together different viewpoints. Expose disagreement and clarify where there needs to be agreement. Example the Delphi method.
- Web 2.0 trust is not that different from trust when a spokesperson stands in front of the camera. We still need to deliver the message. The reputation will build as you deliver the message.

What are the requirements to achieve this?

- Need to understand the technology and its uses better.
- We should be doing this, we need to be doing this, if we don't get on board, we won't be able to effectively do our jobs.
- Best practices
- Research approaches
- Solid examples
- Data sets
- Trust but verify. Don't blindly accept everything. Need to have mechanisms to assist. Also need to provide information that public can trust.
- Truth clusters – errors scatter. General strategy to monitor (traffic and key words) multiple streams of data, sites and systems. When we see the same chatter in multiple channels, send resources to verify. Use common sense.

- The current systems do not accurately accomplish the bridge between collaboration, coordination and cooperation. We need to not accept that social network systems are not designed to meet all our needs. They may need to evolve with our input.
- We need to define what the requirements are – they may be expressed differently by individuals, jurisdictions or organizations.
- Different people need different structures to use and share information. Recognize that the users are going learn as the go. Ways to structure the information and increase the reliability and effectiveness. The users will then provide the updates within the system that provides the most value to them and other contributors. It has to be two-way conversation.
- Several channels we can explore through social media / networking. Stay engaged with community on a daily basis to build that relationship. Then the trust is there when emergencies unfold. Bring clarity to the chaos.
- Find the best tools for preparedness and prevention. Which categories of social media tools should be used for different objectives?
- How can we leverage the public? They fit into the preparedness and prevention area.
- Define what we want from Web 2.0. It boils down to resiliency. We have the opportunity to expand upon systems. Individuals, family, community, state, nation, international (6 levels of resiliency). It is a shared responsibility among these different levels.
- Solutions need to be practical and applied.
- Systems or applications that collect and display geographic clusters that indicate a common thread that makes sense to accept as truth.
- Want a diverse set of sources and a system to tie together the common threads.
- The first reports from individuals will be to their family and their own social networks. How do we mine that information?
- Need to analyze the range of the errors in information to be able to determine what can be discarded.
- Get familiar with the tools and pick and choose which ones from the suite of tools that can be applied during emergencies. Some federal agency (DHS) needs to fund and support the development of tool set.
- Virtual USA, Google Sketch up, research existing tools and find common benefits and desired (but not yet developed) benefits.
- Define: social networking for what? People are using web 2.0 for their own purposes

1. Get message out;
2. Informal inbound requests;
3. Monitoring what is happening in communities like a sensor;
4. How organizations can use technology to collaborate with other organizations.

What partnerships need to be established?

- Broaden networks to achieve collaboration from all directions

- How do I get direction from govt? Tell us what you want? Need to take a broad view and express requirements to technology developers, network systems and public.
- Need to train people to be good observers. Involve them in the planning. Allow them to function as a group.
- About 1/3 of population using Web 2.0 technologies. But we have about 90% or HLS practitioners are not using it. How do we raise the level of engagement within the sector?
- Make a list of type of information we have and need. Develop a protocol for how someone can provide and plug into the protocol. It could be an individual, group, organization, etc. Once the protocol is stable, a developer could pick it up and run with it to simplify the process.
- HLS / EM communities need to partner with technology and network scientists to identify their requirements (beyond the capabilities of existing social media tools) and let the technology developers help align systems to meet the needs.

What collaborative bodies need to be formed?

- Need to build relationships before we can share information.

What funding sources are required?

- Technology is cheap. It's figuring out what you want it to do that is expensive.

What other types of resources are needed to advance our adoption, understanding and the utility of these new forms of communication?

- Need indicators that we regularly track. Word clouds.
- Need to leverage the power of what people are using and will continue using. Cell phones as sensors and more dynamic information systems (temperature readings, blackberry or iphone network systems).
- Need guidelines, a primer on how to use it effectively. Need an educational component. Teach us how. But let agencies use it to compliment existing tools or needs.
- How do emergency managers want the public to access information about evacuations, boil water orders, etc.
- Given the limitations of resources of EM / HLS practitioners, need to have protocols of how to put information out. And have developers work around them to provide value.
- Define the use of information for the basis of mobilizing actions. Identify the thresholds for actions.
- Make more focused resource allocation decisions based upon triggers. What are the triggers?
- Gov't has a hard time throwing away the tools that don't work. But we need to adapt quicker to harness Web 2.0 possibilities.

Summary from yesterday from facilitators: How do we trust info? How do we gain trust of people using social media? How do we gain trust in government? We must remember volume and repetition of information does not equal truth. There was general agreement to think differently – adapt, change, learn. The problem is when people say "you must come around to my point of view" – we must find a way to compromise. Examples of

social media helping public safety – need clearinghouse of smart practices. The horse is already out of the barn so lets move forward.
Summary from participants: 1. Trust but verify (never take information for granted) 2. Be trustworthy but verifiable and 3. truth clusters and error scatters. Important to have a strategy for verifying information (monitoring multiple social media outlets—traditional media, radio, twitter, facebook, etc.). Practitioners understand this is a good tool, but monitoring doesn't always translate easily into resource management (deployment of officers, staging of equipment, etc.).

- Cooperation, coordination and collaboration are different things – cooperation is where we work together, coordination is where we plan together and collaboration is working together on the same issue. We shouldn't be locked into any one social medium – different tools will do different things.
- Trust. This is more than web 2.0 – there is underlying trust that must be built over time.
- The amount of structure or command and control depends on the participants in an emergency and the dynamics of the incident itself. The answer may not be yes or no when it comes to social media, but a multi-layered, channeled approach.
- Trust v. bad guys. Do we use certainly technologies because bad guys use them – sure.
- We need to focus more on the capabilities to use social media in the prevention and preparedness arenas. Practitioners really need to identify what it is they want from social media – for some it is community resilience (individual, family, neighborhoods/community, state, national international). Share responsibility for public safety. Information must be easily understood and applicable. This the larger philosophical issue.
- We not only need to verify information, but we need to be aware of what information might be lacking – is there a certain geographical area or a certain population you haven't heard from. The goal is not just to interpret what you have but seek out what you do not.
- We acknowledge and accepts there are component parts of a system that address the four pillars of homeland security. We are now focus upon this constellation of web 2.0 that may have an impact on these elements. We not throwing out how we usually do business, but know that web 2.0 has a role. What can it do, what part can it play and what is its potential for the future?
- Problem – we acknowledge the worthiness of web 2.0, but 90 percent do not use it.

Does social media fit within NIMS?
Provide practitioners guidelines as to what you can and cannot do with social media applications. They want a "how to" guide. It's fine that we're going to embrace the topic, but teach me how to do it. Need to develop a "plug and play" approach. **Who is going to do this?** Most (85%) law enforcement agencies are small and need to know how tools can be used on a day to day basis.
Self interest vs. organizational interest. 1. organizations can use social networks to get their message out 2. formal inbound requests from citizens to organizations 3. monitoring what is going on (sensor networks) and 4. communicate, coordinate and

collaborate with other organizations. Its about relationships – affiliations with other people (family, friends).
The web is really the only example of interoperability that exists today. You have to be able to pull in participants that can provide photos, narrative, subject matter expertise, etc. and make them a part of incident management.
There will continue to be new tools and new uses – at no level are we going to be able to chase after these things. Protocols are more important and could be applied to whatever the technology of the day is.
Practitioners should make a list of what information they think others might want. What is a very simple protocol for posting that information on a web site. Keep framework very simple – it will last. **The system is not as important and the protocols and guidelines.**
Web 2.0 fills an existing gap and provides value for the users. The practitioners must identify their gaps and requirements.
We must get closer to usable, actionable information.

Key:	Trust 0/13 Experimentation 2/7 Policy 4/3 Relationships 0/7 "How To" 0/15

D. CODED OGMA NOTES FROM THIRD ROUND ROBIN

Technology-Network Science and Media

Key issues:

1. Trust (expertise, teams, groups)
2. Processes
3. Protocols (user guide, share smart practices)
4. Templates
5. Perspective (what may seem simple to some may be complex to others)
6. Enablers (example: technology sector must enable ability to analyze volumes of data)
7. language (event local but response is global) the lack of a common language can create barriers.
8. Design principles
9. lowest common denominator – what is the most basic thing that people need in language and technology? (this is what makes twitter so appealing)
10. Experimentation
11. Information quality

12. Innovation
13. measurement/outcomes

Other:

- Need to develop frame of (processes) and training for users at all levels
- Slowly changing organizations are trying to link themselves to a quickly changing technology environment.
- There is no incentive for the tech community to partner with practitioners
- Communities of practice develop very specific definitions to help facilitate a common language. Must reduce/eliminate ambiguity. We agree as a group that clarity is important.
- Be very careful about broad statements that a certain sector doesn't "need" information.
- Remember if we try to solve the world's problems, we won't solve any. We need to focus on where we can make a difference.
- In an emergency, people will use what they always use – they will not use something new.
- If you want to advocate the use of a technology you must use it.
- It is difficult for the private sector to make an investment in emergency response because it is so episodic – there must be a link to daily life.

Solutions:

1. design principles
2. processes
3. protocols
4. templates
5. syntax
6. approaches to context
7. experimentation
8. money, time and training
9. measurement/metrics

What do we need to do and how do we do it?

1. Investment in more wireless, broadband infrastructure
2. Improve collaboration (share tools, smart practices)
3. Statement of value – tell a story
4. Use social media to bring people into the mission of emergency preparedness
5. Focus on small steps – can we train people how to report info, can we train them how to take photos, train people on collecting damage assessment info
6. Need to be able to use tools (many do not have access to web 2.0 technologies at work)
7. Provide training and education ("how to" guide)
8. leverage a common knowledge base

Key Issues

- Trust
- Processes
- Open Protocols

- When you try to get a team together there is a question of trust and expertise? What about the collaborative piece done on SharePoint and Wikipedia? Media Findings:
- Method: Push - Pull - Mobilize
- All parties need a common language to discuss Web 2.0 (Syntax)
- mcmullinja #ogma Technology Groups Focus - 1) Adoption of Technology 2) Innovation 3) Critical Infrastructure 4) Information Quality. RT @TimOBrienNYT: RT @riparian Twitter, Facebook "gold mines" to social engineers/organized crime, IBM security guy just told me #ogma Issues for Network Science/Media and Technology
- Humility
- Incentive
- Trust
- Enablers
- Simple
- Clarity
- Real World
- Approaches to Context
- Preocesses
- Protocols
- Template
- Syntax
- Set of Principles
- Measurements and Metrics
- Government organizations need access to Web 2.0 Tools.
- Once the emergency begins people will use what they are used to using. Your more likely to find advanced technology in state or local than you will in the Federal Government. You can't move forward without measurements and metrics. The Science of Muddling Through What needs to be done? What do we need to invest in?
- Invest in Infrastructure.
- Wireless
- Broadband
- Improve Collaboration
- Enable exploitation of Web 2.0
- Provide Training and Education
- Groups to identify examples
- Share Information

- Get the information out there and let the people decide what to do with it.
- If the government wants infrastructure then the government has to be pay for it.

Practitioner – Behavioral Science

What do we know and see in practice now?

- Florida State using YouTube to publish sit reports. We provide status and updates on information they find useful. Provide information we think we need to disseminate. Flash reports – situation dependent that shares the relevant info people need to know. This helps achieve transparency.
- Virginia Tech use of Facebook for collective intelligence by distributed systems to share details. Question: How did it influence people who used it? How is behavior changed by technology?
- Studies exist about Virginia Tech and California Wildfires.

What Challenges exist?

- People don't know how to access information among so many different sources.
- People / PIOs in the JICs are not familiar with social media (i.e. Cal wildfires). Didn't know what to look for. Studied whether or not there is accuracy of information, reliability, barriers. But, there has not been a lot of attention focused on adoption of social media by govt agencies / PIOs.

What requires further study, analysis, and exploration?

- Need to define the target audience of daily situational information.
- How do we reach the intended audience? If we reach them, will this improve the relationship? Will it foster better more timely decision making?
- Use social networking tools to build community resiliency and preparedness.
- Determine how the generation gap influences where we are at and how to move forward.
- Social scientists need to show us how and why this matters.
- What are the obstacles for practitioners to use Web 2.0 technologies?
- Engage expertise in social science field to verify strategies. Help build experiments to determine which instruction and method is most effective.
- Is there any study on how technology influences how people react before, during and after an emergency? Does it lead to behavior change?
- Many dinosaur programs that are receiving a large amount of funding need to re-analyzed and divert those resources to new areas.

What are the requirements to achieve this?

- Need to continue the coordination and collaboration.
- Define the key questions and pressing issues.
- Define the priorities of initiatives.
- Determine the next steps for a positive impact to reach tangible outcomes.
- More dialogue is needed.
- The practitioner community needs to pay attention to research being conducted and already published.
- Initiate workshops with practitioners and researchers to identify needed research and to present findings of current research.
- Incorporate an element of web 2.0 technologies to share information within the National Level exercise in Las Vegas.
- Develop a sense of preparedness in communities – this is a widely recognized objective of practitioners. We need to find the right web 2.0 technologies to engage citizens in productive manners to build culture of preparedness. We need social scientists to tell us what are we doing wrong about crafting the message.

- Need to allow practitioners to feel empowered on how to correct invalid information.
- Take advantage of the interactive nature of web 2.0 technologies. Sparking incentives for community members to take actions and become more involved to build community resiliency.
- Use social scientists to help us construct and package messages to influence the behaviors we want to see in place.
- How do we integrate social media into our ICS systems? How do we get our own people engaged? Where does it fit?
- Need research that can be put into place. Message content that leads to actions. Need to incorporate concrete experience. Seeing is believing. Show us the piece that creates understanding about the practical application of why they should act.
- Would like to see academia make their research more accessible.
- Keep reports brief and simple to understand – one-pagers that can be digested by layperson.

What partnerships need to be established?

- Practitioners need to communicate what type of research they want. What questions do they want answered. Then partner with the academic community and social and behavioral scientists.
- Do outreach through non-peer reviewed journals. There is a disconnect between the academic publications versus what the practitioners are reading.
- Research of web-based gaming and analysis of applicability in public education for emergency response. More research on engagement of public through virtual worlds and gaming. It would be a significant change. Too difficult to distill and talk about these tools within the emergency management community.
- Need to effectively measure behavior change. Are our actions and outreach making any difference?

What funding sources are required?

- Academia needs funding to tackle the research needs.

Key:	Trust 9/2 Exercise/Experimentation 4/5 Research/Best practices 2/5 Application 15/5

E. CODED OGMA NOTES FROM FINAL REPORTS

1. Key Issues by Discipline

Technology

- Adoption of Technology
- Innovation
- Experimentation
- Too much information inbound to single responder through Web 2.0 Apps.
- Numerous Web 2.0 Apps (Facebook, MySpace, Qik, Wikipedia, etc.)
- Authentication
- Data Assurance
- Portable Identity
- Standards Compliance
- Interoperability at high-level.
- Information Quality

Behavioral Science

- Lack of clarity regarding what are the issues and how we define them.
- We have yet to define web 2.0
- Need to clarify research objectives.
- Different objectives of different groups/audiences/stakeholders

Network Science and Media

- Policy
- Capturing existing examples of Web 2.0 utilization and sharing with others (sharing best practices)
- Knowledge sharing
- Application of technology – push, pull and mobilize
- Infrastructure needs
- Education
- Protocols
- Trust
- Variety of tools

Practitioners

- Trust – how do we develop it?
- Two way information needs

- Ability to correct information
- Different strategies in how to effectively use social media. Who owns the initiative? Many stakeholders and many different points of view on how to proceed.
- Decision making is intuitive to come from the field. Tools that are predictive are helpful.
- Whether we embrace Web 2.0 or not, the public is using and will drive the need for HLS /EM to participate.
- Privacy is a huge issue, especially if you are monitoring. Coordinate with record retention laws.
- Have we framed the issue well? Can we more effectively utilize the technology potential? What is our relationship with the web world?
- Fight the tendency to pose solutions prior to understanding the full issue (web 2.0).
- Articulate the theory of the business. Define the why, which will determine the how and the what.

Key: Adoption/Implementation of technology
Issues of Trust
Strategy/Polcy
Numerous Tools/Users
Clarity/Definition of Topic

2. Suggested Players/Participants by Discipline

Technology

- Media
- Government (Federal, State, Local, Tribal, etc.)
- Industry Group (if no industry group, target individual companies)
- Public safety organizations
- Target groups that can get things done

Behavioral Science

- "Translator" to translate the requirements (S&T)
- Practitioners as advisors to Researchers
- Industry
- Universities

Network Science and Media

- Congress
- Local public safety practitioners
- Professional associations
- Volunteer organizations, NGO's
- Neighborhood watch/CERT
- DHS
- Public Health
- Academia
- Media
- Open source software developers

Practitioners

no list offered

Key:	Private Sector/Industry
	Public Safety
	Academia

3. Obstacles/Enablers by Discipline

Technology

Obstacles

- Adoption
- Awareness
- Security Policies
- Fear of technology and accessiblity
- Inconsistent Web 2.0 guidance from government
- Changing fads
- Gaps for underprivileged (Accessibility) Lack of inclusivity. Subsidize.
- Need champions to push this along (tech capable)
- Politics
- We need to know what we are trying to do
- Requirements in public safety community do not always work
- Sometimes end users do not know capabilities that exist

- How do you show the responder what is possible so that they can define their needs.
- You need to get to "Robust Statement of Needs"

Enablers

- New Generation (The Millennials) are "growing up online."
- Politics
- Mechanism for confluence of interest
- Engaged and passionate citizens
- Need money

Behavioral Science

- Need to address incentives
- Research Grants that make explicit the need to include research
- Research funding by NSF has moved toward the theoretical
- Policy, Strategy and Funding

Network Science and Media

- Obstacles
  - security driving policy
  - funding
  - culture
  - technical dynamism
- Enablers
  - Cost
  - youth, demographics
  - knowledge base,
  - education
  - media
  - open protocols, open systems

Practitioners

no list offered

Key: Funding
Youth
Security
Education

4. Potential Solutions by Discipline

Technology

- Exercises
- Experimentation
- Co-production
- Competition to develop useful applications
- Apps for democracy example
- Give developers the problem and then let folks solve it.
- Annual prize for needed solutions
- Raise the issue to the following orgs:
    - Build Awareness
    - Media
    - Government (Federal, State, Local, Tribal, etc.)
    - Industry Group
    - Public safety organizations
- Money

Behavioral Science

- Pilot studies, research studies
- Translate research into practice
- Create new distribution channels
- Involve practitioners early in the research process

Network Science and Media

- Policy – mechanisms to educate people "at the top", better describe requirements, get a sense of value and communicate it, beta testing
- Sharing – clearinghouse, community of champions, research, cross pollination for practitioners, technical evangelism
- Knowledge – pilot projects/test bed demonstration, exercises, mandate use of Web 2.0 among own teams, workshops, use social media to share knowledge, enhance outreach to Web 2.0 providers
- Application – develop a construct for application (our suggestion is push, pull and mobilize), goal directed, definition for public safety use, functional requirements, user requirements
- Infrastructure – craft procurement standards, inventory of who uses what, identify needs, risk assessment, clearinghouse for currently useful tools to access social media, culture of rapid change

- Education – "how to" guide for all users and leaders, document examples of use, develop formal training, utilize existing libraries, use train-the-trainer concept for delivery, independent study, CERT is good starting point for educational outreach, incorporate Web 2.0 in all relevant training activities.

Practitioners

- Identification of policies or best practices around roles and responsibilities.
- What type of social networking sites can we build from a trusted source.? Why can't we move into the area from a Homeland Security perspective and create our own. A centralized source would be beneficial.
- Develop "communities of practice" to provide guidelines for organizations.
- Find the right application for social networking tools
- Need to develop a set of rules on how to deal with the new issues that arise.
- Initiatives will require a comprehensive legal review.
- Develop success stories of best practices – provides the real world examples of a practical application. Clearly articulate to all stakeholders the case and not make assumptions of validity.
- Need to develop protocols for what information needs to be shared and how it will be shared.
- Need to integrate existing tools with new dynamic tools. Develop code of conduct for usage of various tools.
- Look to social scientists to help develop message design and delivery.
- Need to communicate our requirements to the technology sector then engage with them on how to develop tools. Also engage with technology about security and firewall issues.
- Involve individuals and the community – this is critical. Recognize the investment of the community of users that value these tools.
- Need to educate and train the HLS community to better understand Web 2.0
- Integrate the solution into existing DOC / EOC structures. Determine how it fits into ICS.

Key: Exercises
Share Smart Practices
Education
Standards
Collaboration

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Altshuller, S. & Benbunan-Fich, R. (2008). In Search of Trust for Newly Formed Disaster Recovery Teams. *International Journal of Technology, Policy and Management,* 8 (4), pp. 383–400.

Bach, R. & Kaufman, D. (2009). A Social Infrastructure for Hometown Security: Evolving the Homeland Security Paradigm. CNA Corporation.

Brafman, O. (2006). *The Starfish and the Spider.* New York, NY: Penguin Group (USA), Inc.

Byrne, M. & Whitmore, C. (2008). Crisis Informatics. *International Association of Emergency Managers Bulletin.*

Collins, H. (2009). *Emergency Managers and First Responders Use Twitter and Facebook to Update Communities*. Retrieved on August 2, 2009 from http://www.emergencymgmt.com/safety/Emergency-Managers-and-First.html

Conroy, A. (2008) *What is Going to Move the Needle On Citizen Preparedness?* Masters Thesis, Naval Postgraduate School, Monterey, CA.

Council for Excellence in Government. (2004). *We the People: Homeland Security from the Citizens' Perspective.*

Covey, S. (2006). *The Speed of Trust: the One Thing That Changes Everything*. New York, NY: Simon & Schuster, Inc.

Drapeau, M. & Well, L. (2009). *Social Software and National Security: An Initial Assessment.* Fort Lesley J. McNair, Washington, DC: Center for Technology and National Security Policy, National Defense University.

Dugeon, C & Hogan, K. (2009). *Social Media and Public Engagement in Emergency Management: Being Part of the Conversation* [PowerPoint slides]. Charlotte, NC: National UASI Annual Conference.

Federal Emergency Management Agency. (2009). *Basic Guidance for Public Information Officers*.

Flynn, S. (2008). America the Resilient: Defying Terrorism and Mitigating Natural Disasters. *Foreign Affairs*. Retrieved June 12, 2008, from http://www.foreignaffairs.com/articles/63214/stephen-e-flynn/america-the-resilient

Flynn, S. (2007). *The Edge of Disaster*. New York, NY; Random House.

Forest, J. (2006). The Role of Everyday Citizens in Homeland Security. Nieman Watchdog Web Site. Retrieved Feb. 27, 2009, from http://www.niemanwatchdog.org/index.cfm?askthisid=232&fuseaction=Ask_this.view

Gallup Poll. (2009). Retrieved July 20, 2009, from http://www.gallup.com/poll/113638/Nearly-Half-Americans-Frequent-Internet-Users.aspx

Gerencser, M., Van Lee, R., Napolitano, F. & Kelly, C. (2008). *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*. New York, NY: Palgrave MacMillan.

Glass, T. (2001). Understanding Public Response to Disasters. *Public Health Reports/2001 Supplement 2/Volume 116*, Baltimore, MD: John Hopkins University, Bloomberg School of Public Health.

Gorman, S. (2003). *Fear Factor: Beyond a Panic-Driven Approach to Homeland Security.* Retrieved Feb. 27, 2009, from http://www.govexec.com/story_page.cfm?filepath=/dailyfed/0503/051603nj1.htm&oref=search

Gross, G. (2003). *Coalition Uses Web for Emergency Notification*. InfoWorld. Retrieved on Sept. 23, 2008, from http://www.infoworld.com/archives/article08/20/03

Hayes, G. & Papworth, L. (2008). *Social Media Campaign*. Retrieved on July 30, 2009, from http://www.flickr.com/photos/garyhayes/2973684461/

Homeland Security Council. (2007). *National Strategy for Homeland Security*.

Jaeger, P., Shneiderman, B,; Fleischmann, K., Preece, J., Qu, Y. & Wu, P. (2007). *Community Response Grids: E-government, Social Networks and Effective Emergency Management*. College Park, MD: University of Maryland, College of Information Studies.

Kendra, J. & Wachtendorf, T. (2006) *Improvisation, Creativity and the Art of Emergency Management* (Preliminary Paper #357). Newark, DE: University of Delaware Disaster Research Center.

Larsen, J. & Pravecek, T. (2006). Comparative U.S. – Israeli Homeland Security. *Counterproliferation Paper No. 34*, Maxwell Air Force Base, AL: USAF Counterproliferation Center.

Larsen, R. (2007). *Our Own Worst Enemy.* New York, NY: Grand Central Publishing.

Lehrer, E. (2001). Citizen Soldiers: What the U.S. Can Learn from Israel About Fighting Terror. *American Enterprise*.

Light, P. (2005). *Preparing For the Unthinkable: A Report on the State of Citizen Preparedness*. New York, NY: New York University, Center for Catastrophe, Preparedness and Response.

McCarter, M. (2009). Social Networks to the Rescue. *Homeland Security Today Magazine.*

Mehrotra, S., Butts, C., Kalashnikov, D., Venkatasubramanian, N., Altintas, K., Hariharan, R., Lee, H., Ma, Y., Myers, A.,Wickramasuriya, J., Eguchi, R. & Huyck, C. (2004). *CAMAS: A Citizen Awareness System for Crisis Mitigation*. Paper presented at the ACM SIGMOD Conference. Paris, France.

Merari, A. (2000). Israel's Preparedness for High Consequence Terrorism. *BCSIA Discussion Paper 2000-30, ESDP Discussion Paper ESDP-200-02*. Cambridge, MA: Harvard University, John F. Kennedy School of Government.

National Commission on Terrorist Attacks. (2004). *9/11 Commission Report*. New York, NY: W.W. North & Company Ltd.

O'Reilly, T. (2006). *Web 2.0 Compact Definition: Trying Again*. Retrieved July 20, 2009, from http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html

Palen, L., Vieweg, S., Sutton, J., Liu, S. & Hughes, A.(2007). Crisis Informatics: Studying Crisis in a Networked World. Boulder, CO: University of Colorado.

Putnam, R. (2000). *Bowling Alone*. New York, NY: Simon & Schuster.

Ripely, Amanda. (2008). *The Unthinkable*. New York, NY: Crown Publishing.

Shaw, R. (2005). *A Private Sector Vision for Broadband Emergency Communications. IP Telephony*. Retrieved Sept. 24, 2008, from http://blogs.zdnet.com/ip-telephony/?p=749

Social media. (n.d.) Retrieved August 22, 2009, from Wikipedia: http://en.wikipedia.org/wiki/Social_media

Spadanuta, L. (2007). Disaster Preparedness 2.0, *Security Management*, 51(12).

Stephenson, D. & Bonabeau, E. (Feb. 2007). Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy. *Homeland Security Affairs III, no. 1*. Retrieved June 23, 2008, from http://www.hsaj.org/?article=3.1.3

Stephenson, D. (2007). Networked Homeland Security: Transforming the Public Into Full Partners in Terrorism and Natural Disaster Preparation and Response by Capitalizing on Personal Communication Devices and the Science of Emergency Behavior. *Homeland Security Institute*.

Sutton, J., Palen, L. & Shklovski, I. (2008). Backchannels on the Front Lines: Emergent Uses of Social Media in the 2007 California Wildfires. Boulder, CO: University of Colorado.

Tucker, J., (2003). *Strategies for Countering Terrorism: Lessons from the Israeli Experience.* Retrieved on April 8, 2009, from http://www.homelandsecurity.org/journal/Articles/tucker-israel.html

Van Leuven, L. (2009). *Optimizing Citizen Engagement During Emergencies Through the Use of Web 2.0 Technologies*. Master's Thesis, Naval Postgraduate School, Monterey, CA.

Vieweg, S., Palen, L., Liu, S., Hughes, A. & Sutton, J. (May 2008). *Collective Intelligence in Disaster: Examination of the Phenomenon in the Aftermath of the 2007 Virginia Tech Shooting*. Boulder, CO: University of Colorado.

Wolf, G. (2008). Reinventing 911: How a swarm of networked citizens is building a better emergency broadcast system. *Wired*. Retrieved June 24, 2008, from http://www.wired.com/wired/archive/13.12/warning_pr.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Steven C. Bailey, Director
   Pierce County Department of Emergency Management
   Tacoma, Washington

4. Ken Parrish
   Pierce County Department of Emergency Management
   Tacoma, Washington

5. Tom Miner
   Pierce County Department of Emergency Management
   Tacoma, Washington

6. Thomas Symonds
   Pierce County Department of Emergency Management
   Tacoma, Washington

7. Hunter George
   Office of the Pierce County Executive
   Tacoma, Washington

8. Ann Lesperance
   Pacific Northwest National Labs
   Seattle, Washington